PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Assistant Commissioner for Patents
United States Patent and Trademark Office
Box PCT
Washington, D.C.20231
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing: 03 August 2000 (03.08.00)	
International application No.: PCT/JP99/01350	Applicant's or agent's file reference: GFS0007
International filing date: 18 March 1999 (18.03.99)	Priority date: 28 January 1999 (28.01.99)
Applicant: YASUKURA, Yutaka	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International preliminary Examining Authority on:

16 February 2000 (16.02.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer: J. Zahra Telephone No.: (41-22) 338.83.38

Form PCT/IB/331 (July 1992)

3432195

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

SEKI, Masaharu
Seki Patent Office
Saiwai building 4th floor
4, Gobancho
Chiyoda-ku
Tokyo 102-0076
JAPON

Date of mailing (day/month/year)
09 April 2001 (09.04.01)

Applicant's or agent's file reference
GFS0007

IMPORTANT NOTIFICATION

International application No.
PCT/JP99/01350

International filing date (day/month/year)
18 March 1999 (18.03.99)

1. The following indications appeared on record concerning:

[X] the applicant [X] the inventor [ ] the agent [ ] the common representative

Name and Address
YASUKURA, Yutaka
15-22, Katsutadai-minami 2-chome
Yachiyo-shi
Chiba 276-0025
Japan

State of Nationality: JP
State of Residence: JP
Telephone No.: 81-474-86-5589
Facsimile No.: 81-474-84-5670
Teleprinter No.:

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address
YASUKURA, Yutaka
11-13-506, Hatagaya 1-chome
Shibuya-ku, Tokyo-to 151-0072
Japan

State of Nationality: JP
State of Residence: JP
Telephone No.: 81-474-86-5589
Facsimile No.: 81-474-84-5670
Teleprinter No.:

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland

Facsimile No.: (41-22) 740.14.35

Authorized officer
Y. KUWAHARA

Telephone No.: (41-22) 338.83.38

Form PCT/IB/306 (March 1994)

003960234

Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference GFS0007	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/JP99/01350	International filing date (*day/month/year*) 18 March 1999 (18.03.99)	Priority date (*day/month/year*) 28 January 1999 (28.01.99)
International Patent Classification (IPC) or national classification and IPC G09C 1/04, 1/00, H04L 9/32		
Applicant YASUKURA, Yutaka		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☐ Certain defects in the international application
- VIII ☒ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
16 February 2000 (16.02.00)	14 November 2000 (14.11.2000)
Name and mailing address of the IPEA/JP Facsimile No.	Authorized officer Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

national application No.
PCT/JP99/01350

I. Basis of the report

1. With regard to the **elements** of the international application:*

☐ the international application as originally filed

☒ the description:

pages 1,3-5,8-18, as originally filed

pages _____, filed with the demand

pages 2,6,7,19,20, filed with the letter of 12 July 2000 (12.07.2000)

☒ the claims:

pages 3,5,6,11, as originally filed

pages _____, as amended (together with any statement under Article 19

pages 2, filed with the demand

pages 1,4,7,10, filed with the letter of 12 July 2000 (12.07.2000)

☒ the drawings:

pages 1-11, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

☐ the sequence listing part of the description:

pages _____, as originally filed

pages _____, filed with the demand

pages _____, filed with the letter of _____

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in written form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☐ the description, pages _____

☒ the claims, Nos. 8,9,12,13

☐ the drawings, sheets/fig _____

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* *Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).*

** *Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-7,10,11	YES
	Claims		NO
Inventive step (IS)	Claims		YES
	Claims	1-7,10,11	NO
Industrial applicability (IA)	Claims	1-7,10,11	YES
	Claims		NO

2. Citations and explanations

Claims 1 to 5, 10, 11

Document 1 [JP, 61-107375, A (Fujitsu Ltd.), 26 May 1986 (26.05.86), full text, Figs. 1 to 4] describes a method for securing safety of electronic information wherein an input data is divided into a plurality of blocks, block transposition is conducted by a random transposition table and element transposition is conducted by an element transposition table, and each divided block is merged, resulting in an encrypted text including all elements; and through the exact reverse of this processing decryption is conducted. In light of the fact that in this method each table is created from random data based on a key table, it would be obvious to a party skilled in the art that this table corresponds to a type of section key required for encryption or decryption.

Document 2 [JP, 60-247683, A (Mitsubishi Electric Corp.), 7 December 1985 (07.12.85), page 1, lower right column, line 2 to page 2, upper left column, line 9, Figs. 1 to 3] describes art wherein an original information array is divided into a plurality of encrypted information pieces and dispersed and stored with the key therefor.

It would be obvious to a party skilled in the art, in order to eliminate harm from a third party with bad intentions, to adopt the art described in document 2 as the encrypted data and key storage method in the method for securing safety of electronic information described in document 1.

Claims 6, 7

Document 3 [JP, 63-225840, A (Yokogawa-Hewlett Packard, Ltd.), 20 September 1988 (20.09.88), page 2, lower left column, line 19 to page 3, lower right column, line 1, Figs. 1 to 6] describes art for guaranteeing the originality of a message by making the global MAC message authentication code for the entire information comprising a plurality of blocks computable by merging the block MACs calculated for each MAC.

Document 4 [JP, 3-151738, A (Hitachi Ltd.), 27 June 1991 (27.06.91), page 4, upper left column, lines 14 to 20, page 4, lower right column, line 15 to page 5 upper right column, line 10, Figs. 1 to 9] describes art for guaranteeing the originality of data by making verifiable alteration of file contents through the division of file data and the logical computation of compressed text created for the divided pieces of file data.

It would be obvious to a party skilled in the art, in order to eliminate harm from a third party with bad intentions, to adopt, while giving consideration to the well-known art described in documents 3 and 4, the art described in document 2 as the encrypted data and key storage method in the method for securing safety of electronic information described in document 1.

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

The inventions described in the claims is understood to define art whereby, through the storage of a very small portion of transmitted electronic information, proof is made for the whole said electronic information. However, it currently has not been mathematically proven that, just by considering a very small portion of electronic information, the authenticity (for example, that the information has not been tampered with) can be proven with certainty, nor does the specification offer such proof.

Therefore, the specification does not sufficiently support the notion that the inventions of this application possess the technological concept of using only a very small portion of electronic data as a means to confirm the authenticity of the electronic data.

16T
10K

特　許　協　力　条　約

PCT

国際予備審査報告

(法第１２条、法施行規則第56条)
〔ＰＣＴ３６条及びＰＣＴ規則70〕

出願人又は代理人の書類記号　ＧＦＳ０００７	今後の手続きについては、国際予備審査報告の送付通知（様式ＰＣＴ／ＩＰＥＡ／４１６）を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ９９／０１３５０	国際出願日 (日.月.年)　１８．０３．９９	優先日 (日.月.年)　２８．０１．９９
国際特許分類（ＩＰＣ） Ｉｎｔ．Ｃｌ⁷　Ｇ０９Ｃ１／０４，Ｇ０９Ｃ１／００，Ｈ０４Ｌ９／３２		
出願人（氏名又は名称） 保倉　豊		

1．　国際予備審査機関が作成したこの国際予備審査報告を法施行規則第57条（ＰＣＴ３６条）の規定に従い送付する。

2．　この国際予備審査報告は、この表紙を含めて全部で　5　ページからなる。

☐　この国際予備審査報告には、附属書類、つまり補正されて、この報告の基礎とされた及び／又はこの国際予備審査機関に対してした訂正を含む明細書、請求の範囲及び／又は図面も添付されている。
（ＰＣＴ規則70.16及びＰＣＴ実施細則第６０７号参照）
この附属書類は、全部で＿＿＿＿＿＿ページである。

3．　この国際予備審査報告は、次の内容を含む。

I　☒　国際予備審査報告の基礎

II　☐　優先権

III　☐　新規性、進歩性又は産業上の利用可能性についての国際予備審査報告の不作成

IV　☐　発明の単一性の欠如

V　☒　ＰＣＴ３５条(2)に規定する新規性、進歩性又は産業上の利用可能性についての見解、それを裏付けるための文献及び説明

VI　☐　ある種の引用文献

VII　☐　国際出願の不備

VIII　☒　国際出願に対する意見

国際予備審査の請求書を受理した日 １６．０２．００	国際予備審査報告を作成した日 １４．１１．００
名称及びあて先 日本国特許庁（ＩＰＥＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	特許庁審査官（権限のある職員）　５Ｗ　４２２９ 青木　重徳　印 電話番号　０３－３５８１－１１０１　内線　４２２９

様式ＰＣＴ／ＩＰＥＡ／４０９（表紙）（１９９８年７月）

国際予備審査報告

国際出願番号　ＰＣＴ／ＪＰ９９／０１３５０

Ⅰ．　国際予備審査報告の基礎

1．　この国際予備審査報告は下記の出願書類に基づいて作成された。（法第６条（ＰＣＴ１４条）の規定に基づく命令に応答するために提出された差し替え用紙は、この報告書において「出願時」とし、本報告書には添付しない。ＰＣＴ規則70.16, 70.17）

☐ 出願時の国際出願書類

☒ 明細書　第 1，3－5，8－18 ページ、　出願時に提出されたもの
明細書　第 　　ページ、　国際予備審査の請求書と共に提出されたもの
明細書　第 2，6，7，19，20 ページ、　12．07．00 付の書簡と共に提出されたもの

☒ 請求の範囲　第 3，5，6，11 項、　出願時に提出されたもの
請求の範囲　第 　　項、　ＰＣＴ１９条の規定に基づき補正されたもの
請求の範囲　第 2 項、　国際予備審査の請求書と共に提出されたもの
請求の範囲　第 1，4，7，10 項、　12．07．00 付の書簡と共に提出されたもの

☒ 図面　第 1－11 ~~ページ~~図、　出願時に提出されたもの
図面　第 　　ページ／図、　国際予備審査の請求書と共に提出されたもの
図面　第 　　ページ／図、　　付の書簡と共に提出されたもの

☐ 明細書の配列表の部分　第　　ページ、　出願時に提出されたもの
明細書の配列表の部分　第　　ページ、　国際予備審査の請求書と共に提出されたもの
明細書の配列表の部分　第　　ページ、　　付の書簡と共に提出されたもの

2．　上記の出願書類の言語は、下記に示す場合を除くほか、この国際出願の言語である。

上記の書類は、下記の言語である　　語である。

☐ 国際調査のために提出されたＰＣＴ規則23.1(b)にいう翻訳文の言語
☐ ＰＣＴ規則48.3(b)にいう国際公開の言語
☐ 国際予備審査のために提出されたＰＣＴ規則55.2または55.3にいう翻訳文の言語

3．　この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際予備審査報告を行った。

☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出された書面による配列表
☐ 出願後に、この国際予備審査（または調査）機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

4．　補正により、下記の書類が削除された。
☐ 明細書　第　　ページ
☒ 請求の範囲　第 8，9，12，13 項
☐ 図面　図面の第　　ページ／図

5．☐ この国際予備審査報告は、補充欄に示したように、補正が出願時における開示の範囲を越えてされたものと認められるので、その補正がされなかったものとして作成した。（ＰＣＴ規則70.2(c)　この補正を含む差し替え用紙は上記１．における判断の際に考慮しなければならず、本報告に添付する。）

国際予備審査報告

国際出願番号　PCT／JP99／01350

V.　新規性、進歩性又は産業上の利用可能性についての法第12条（PCT35条(2)）に定める見解、それを裏付ける文献及び説明

1.　見解

新規性（N）
請求の範囲　1－7，10，11　有
請求の範囲　　無

進歩性（IS）
請求の範囲　　有
請求の範囲　1－7，10，11　無

産業上の利用可能性（IA）
請求の範囲　1－7，10，11　有
請求の範囲　　無

2.　文献及び説明（PCT規則70.7）

請求の範囲1－5，10－11
文献1：JP，61－107375，A　（富士通株式会社）
26．5月．1986　（26．05．86）全文，第1－4図
には、入力データブロックを複数のブロックに分割し、ランダム転置テーブルによりブロック転置処理を行うとともにエレメント転置テーブルによりエレメント転置処理を行い、各分割ブロックを統合することで全てのエレメントが含まれる暗号文を得る一方、この操作と全く逆の処理を行うことでデータが復号できる電子情報の安全確保方法が記載されており、この方法での各テーブルはキーデータに基づいたランダムデータから作成されていることを勘案すれば、該テーブルは暗号化ないしは復号化のために必要な一種のセッション鍵に相当することは当技術分野の専門家にとっては自明なことである。
文献2：JP，60－247683，A　（三菱電機株式会社）
7．12月．1985　（07．12．85）
第1頁右下欄第2行－第2頁左上欄第9行，第1－3図
には、元の情報列を暗号化された複数個の情報に分割して鍵と共に分散保管する技術が記載されている。
悪意ある第三者からの妨害を排除するために、文献1に記載された電子情報の安全確保方法における暗号化データや鍵の保管技術として、文献2に記載された技術を採用することは、当技術分野の専門家にとっては自明のものである。

請求の範囲6、7
文献3：JP，63－225840，A　（横河・ヒューレット・パッカード株式会社）
20．9月．1988　（20．09．88）
第2頁左下欄第19行－第3頁右下欄第1行，第1－6図
には、複数のブロックからなる情報の本体全体についてのグローバルMACメッセージ認証コードを各ブロック毎に計算されたブロックMACを統合して計算できるようにすることで、メッセージの原本性を補償する技術が記載されている。
文献4：JP，3－151738，A　（株式会社日立製作所）
27．6月．1991　（27．06．91）
第4頁左上欄第14－20行，
第4頁右下欄第15行－第5頁右上欄第10行，第1－9図
には、ファイルデータを分割し、分割した個々のファイルデータに対して作成した圧縮文を論理演算することによりファイル内容の改ざんを検証できることでデータの原本性を補償する技術が記載されている。

Ⅷ.　国際出願に対する意見

請求の範囲、明細書及び図面の明瞭性又は請求の範囲の明細書による十分な裏付についての意見を次に示す。

各請求の範囲に記載された発明は、伝送する電子情報の極く一部のみを保管するだけで当該電子情報の全容について証明できるようにした技術を定義したとも読みとれるが、電子情報の極く一部のみを参酌するだけで、該電子情報が、例えば改竄などを受けていないという、いわゆる真正性を確実に証明可能であることは、現在数学的に証明がなされておらず、また、明細書中においてもそのような証明が記載されていない。

したがって、本願発明が電子情報の極く一部のデータのみを用いて、これを該電子情報の真正性を確認する手段とした技術的思想を有すると十分な裏付けが明細書によりなされていない。

補充欄（いずれかの欄の大きさが足りない場合に使用すること）

第 Ｖ．２ 欄の続き

悪意ある第三者からの妨害を排除するために、文献１に記載された電子情報の安全確保方法における暗号化データや鍵の保管技術として、文献２に記載された技術を文献３、４に記載された周知技術を考慮しつつ採用することは、当技術分野の専門家にとっては自明のものである。

特　許　協　力　条　約

EP US

PCT

国際調査報告

(法８条、法施行規則第40、41条)
〔ＰＣＴ１８条、ＰＣＴ規則43、44〕

出願人又は代理人の書類記号　ＧＦＳ００７	今後の手続きについては、国際調査報告の送付通知様式(ＰＣＴ／ＩＳＡ／２２０)及び下記５を参照すること。	
国際出願番号 ＰＣＴ／ＪＰ９９／０１３５０	国際出願日 (日.月.年)　１８．０３．９９	優先日 (日.月.年)　２８．０１．９９
出願人（氏名又は名称） 保倉　豊		

国際調査機関が作成したこの国際調査報告を法施行規則第41条（ＰＣＴ１８条）の規定に従い出願人に送付する。
この写しは国際事務局にも送付される。

この国際調査報告は、全部で　3　ページである。

☐ この調査報告に引用された先行技術文献の写しも添付されている。

１．国際調査報告の基礎

ａ．言語は、下記に示す場合を除くほか、この国際出願がされたものに基づき国際調査を行った。
☐ この国際調査機関に提出された国際出願の翻訳文に基づき国際調査を行った。

ｂ．この国際出願は、ヌクレオチド又はアミノ酸配列を含んでおり、次の配列表に基づき国際調査を行った。
☐ この国際出願に含まれる書面による配列表
☐ この国際出願と共に提出されたフレキシブルディスクによる配列表
☐ 出願後に、この国際調査機関に提出された書面による配列表
☐ 出願後に、この国際調査機関に提出されたフレキシブルディスクによる配列表
☐ 出願後に提出した書面による配列表が出願時における国際出願の開示の範囲を超える事項を含まない旨の陳述書の提出があった。
☐ 書面による配列表に記載した配列とフレキシブルディスクによる配列表に記録した配列が同一である旨の陳述書の提出があった。

２．☐ 請求の範囲の一部の調査ができない（第Ⅰ欄参照）。

３．☐ 発明の単一性が欠如している（第Ⅱ欄参照）。

４．発明の名称は
☒ 出願人が提出したものを承認する。
☐ 次に示すように国際調査機関が作成した。

５．要約は
☒ 出願人が提出したものを承認する。
☐ 第Ⅲ欄に示されているように、法施行規則第47条（ＰＣＴ規則38.2(b)）の規定により国際調査機関が作成した。出願人は、この国際調査報告の発送の日から１カ月以内にこの国際調査機関に意見を提出することができる。

６．要約書とともに公表される図は、
第　4　図とする。☐ 出願人が示したとおりである。　☐ なし
☐ 出願人は図を示さなかった。
☒ 本図は発明の特徴を一層よく表している。

国際調査報[redacted]　　国際出願番号[redacted]CT／JP99／01350

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁶　G09C1／04, G09C1／00, H04L9／32

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁶　G09C1／04, G09C1／00, H04L9／32

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－1999年
日本国登録実用新案公報	1994－1999年
日本国実用新案登録公報	1996－1999年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 2-259689, A（松下電器産業株式会社） 22.10月.1990（22.10.90） 全文, 第1-6図, （ファミリーなし）	1-13
Y	JP, 60-247683, A（三菱電機株式会社） 7.12月.1985（07.12.85） 第1頁右下欄第2行-第2頁左上欄第9行, 第1-3図 （ファミリーなし）	4, 11-13

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日 01. 06. 99	国際調査報告の発送日　15.06.99
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 青木　重徳　印　5W　4229 電話番号　03－3581－1101　内線　3576

様式PCT／ISA／210（第2ページ）（1998年7月）

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP, 63-225840, A（横河・ヒューレット・パッカード株式会社） 20.9月.1988（20.09.88） 第2頁左下欄第19行-第3頁右下欄第1行, 第1-6図, & GB, 8704883, A & EP, 281225, A & US, 4933969, A & DE, 3889561, C	6-9
Y	JP, 3-151738, A（株式会社日立製作所） 27.6月.1991（27.06.91） 第4頁左上欄第14-20行, 第4頁右下欄第15行-第5頁右上欄第10行, 第1-9図, （ファミリーなし）	6-9
Y	JP, 8-185376, A（株式会社日立製作所） 16.7月.1996（16.07.96） 第2頁第2欄第3-36行, 第3頁第3欄第2-7行, 第6頁第10欄第18行-第7頁第11欄第22行, （ファミリーなし）	13
A	JP, 10-91705, A（株式会社日立製作所） 10.4月.1998（10.04.98） 第2頁第2欄第49行-第3頁第3欄第42頁, （ファミリーなし）	1-13
A	JP, 62-72243, A（富士通株式会社） 2.4月.1987（02.04.87） 第1頁右下欄第5-10行, 第2頁左上欄第15-17行, 第1-2図, （ファミリーなし）	1-13

PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF THE RECORDING OF A CHANGE

(PCT Rule 92bis.1 and Administrative Instructions, Section 422)

To:

SEKI, Masaharu
Seki Patent Office
Saiwai building 4th floor
4, Gobancho
Chiyoda-ku
Tokyo 102-0076
JAPON

Date of mailing (day/month/year)
09 April 2001 (09.04.01)

Applicant's or agent's file reference
GFS0007

IMPORTANT NOTIFICATION

International application No.
PCT/JP99/01350

International filing date (day/month/year)
18 March 1999 (18.03.99)

1. The following indications appeared on record concerning:

[X] the applicant [X] the inventor [ ] the agent [ ] the common representative

Name and Address	State of Nationality	State of Residence
YASUKURA, Yutaka 15-22, Katsutadai-minami 2-chome Yachiyo-shi Chiba 276-0025 Japan	JP	JP
	Telephone No.: 81-474-86-5589	
	Facsimile No.: 81-474-84-5670	
	Teleprinter No.:	

2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:

[ ] the person [ ] the name [X] the address [ ] the nationality [ ] the residence

Name and Address	State of Nationality	State of Residence
YASUKURA, Yutaka 11-13-506, Hatagaya 1-chome Shibuya-ku, Tokyo-to 151-0072 Japan	JP	JP
	Telephone No.: 81-474-86-5589	
	Facsimile No.: 81-474-84-5670	
	Teleprinter No.:	

3. Further observations, if necessary:

4. A copy of this notification has been sent to:

[X] the receiving Office
[ ] the International Searching Authority
[ ] the International Preliminary Examining Authority
[ ] the designated Offices concerned
[X] the elected Offices concerned
[ ] other:

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Y. KUWAHARA
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

(Translation of the First Amendment filed on 16.02.00)

WRITTEN AMENDMENT

(Amendment under the Provision of Patent Law Section)

To: Commissioner of the Patent Office

1. Indication of International Application:

PCT/JP99/01350

2. Patent Applicant

Name: YASUKURA Yutaka

Mail Address: 15-22, Katsutadai-minami 2-chome,
Yachiyo-shi, Chiba-ken, 276-002 JAPAN

Nationality: Japan

Adress: Japan

3. Agent

Name: SEKI Masaharu, Patent Attorney (10434)

Mail Address: Seki Patent Office
Saiwai bldg. 4 Fl.
4, Gobancho, Chiyoda-ku, Tokyo 102-0076
Japan

4. Item to be Amended: Claims

5. Contents of the Amendment: As recited in the separate sheets.

(1) Claims 1, 2 and 12 are amended while the other claims are maintained.

6. List of Annexed Documents: claims one copy

Claims:

1. (As amended) A security assurance method for electronic information, characterized in that an electronic information file is divided into a plurality of information elements; the divided information elements are selected and combined with their order changed to produce two or more information blocks in which all of the information elements are included if all of the information blocks are integrated; division extraction data in which division information of said information elements and formation information of the information blocks are recorded is produced; said information blocks and the division extraction data are stored or transmitted separately so that all of the information may not gather at a time; and when said electronic information is to be utilized, all of said information blocks and the division extraction data are collected and said information blocks are re-divided into the original information elements, re-arranged in the correct order and integrated based on said division extraction data to restore the original electronic information file.

2. (As amended) A security assurance method for electronic information according to claim 1, characterized in that said division extraction data is

stored or transmitted separately by different means from that with which said information blocks are stored or transmitted.

3. A security assurance method for electronic information according to claim 1, characterized in that said division extraction data relating to said information elements is annexed for each of said information elements.

4. A security assurance method for electronic information according to any one of claims 1 to 3, characterized in that said information blocks and the division extraction data are stored into an external storage apparatus to keep the electronic information in said external storage apparatus in security.

5. A security assurance method for electronic information according to any one of claims 1 to 3, characterized in that a plurality of said information blocks are formed, and said blocks are transmitted in a separate state from each other to a recipient together with said division extraction data.

6. A security assurance method for electronic information according to claim 5, characterized in that said division extraction data includes data for confirmation of the originality of said electronic information file.

7. A security assurance method for electronic information

according to any one of claims 1 to 6, characterized in that an information element selected from among said information elements is included commonly into a plurality of information blocks, and when the information elements are integrated, the identity of said information elements included commonly in an overlapping relationship in the different information blocks is verified to confirm the security of the information.

8. A security assurance method for electronic information according to any one of claims 5 to 7, characterized in that further the original of the electronic information to be transmitted is stored; the electronic information restored by the recipient side is sent back; and the electronic information is verified with said original of the electronic information to confirm the identity.

9. A security assurance method for electronic information according to any one of claims 5 to 7, characterized in that further the original of the electronic information to be transmitted is stored; the information blocks received by the recipient side are sent back; and the information blocks are verified with said original of the electronic information to confirm the identity.

10. A security assurance method for electronic information according to any one of claims 5 to 9,

characterized in that at least one of said information blocks and said division extraction data is transmitted to the recipient by second transmission means different from the transmission means for the other electronic information.

11. A security assurance method for electronic information according to claim 10, characterized in that a transfer station is interposed in said transmission means or said second transmission means, and a block of the information to be sent by said transmission means is accommodated into an information package together with destination information and sent to said transfer station, which in turn transfers the information block to said recipient based on said destination information.

12. (As amended) A security assurance method for electronic information according to claim 11, characterized in that said transfer station keeps said information block until a request of said recipient is received.

13. A security assurance method for electronic information according to any one of claims 1 to 12, characterized in that said information blocks obtained by the division of the electronic information file are possessed divisionally by a certification station and

parties concerned, and when said electronic information is to be used, all of said information blocks are collected from said certification station and said parties concerned and integrated to restore the original electronic information.

(Translation of the Reply filed on 12.07.00)

WRITTEN REPLY

To: Shigenori AOKI, Examiner of the Patent Office

1. Indication of International Application:

PCT/JP99/01350

2. Patent Applicant

Name: YASUKURA Yutaka

Mail Address: 15-22, Katsutadai-minami 2-chome,
Yachiyo-shi, Chiba-ken, 276-002 JAPAN

Nationality: Japan

Adress: Japan

3. Agent

Name: SEKI Masaharu, Patent Attorney (10434)

Mail Address: Seki Patent Office
Saiwai bldg. 4 Fl.
4, Gobancho, Chiyoda-ku, Tokyo 102-0076
Japan

4. Date of Notification: May 23, 2000

5. Contents of the Answer

(1) It is alleged in the PCT opinion forwarded May 23, 2000 that the present application lacks in inventive

step. The Applicant submits an Amendment in which the specification and the claims are amended.

The amendment to the specification is made in connection with the amendment to the claims to make the description of the Disclosure of the Invention consistent with the invention as set forth in the amended claims, but does not alter the contents of the application as filed.

(2) Claim 1 as amended is based on Claim 13 before the amendment and defines a security assurance method for electronic information wherein a certification station is interposed to allow confirmation of the genuineness of electronic information. Although the certification station stores only part of electronic information, the genuineness of electronic information possessed by the parties concerned can be confirmed with certainty by the method of division and distribution of electronic information of the present invention. The amendment is made to represent the matters more definitely.

It is to be noted that, in order to make the present invention more definite, it is recited clearly that information blocks in the present invention are such that, "if all of the information blocks are not integrated, then all of the information elements are not

included".

By applying to the certification station the technique of preventing all electronic information from being present at a time in one storage medium or in one transmission path in accordance with the present invention, transmission and storage of electronic information can be performed in security and the load to the certification station can be reduced significantly. Consequently, administration of the certification station with high reliability can be performed economically. Further, information blocks to be integrated do not allow restoration of the entire information in its complete form even if one of them misses, and by using such a division and integration method as just described, the genuineness of an owner of electronic information is confirmed, for example, in such a case that contents are transmitted for on-line sales or electronic information possessed by the parties concerned with a contract is confirmed.

On the other hand, the documents cited in the international search report and the PCT opinion in the international preliminary examination neither teach nor suggest a certification station which utilizes the technique of making it possible to certify the entire

contents of electronic information to be transmitted by storing only a very small part of the electronic information. Also, none of the cited documents discloses the technical idea that a very small part of data is reserved and used as means for confirmation of the genuineness of the electronic information.

Accordingly, the invention as set forth in claim 1 as amended has the inventive step. Further, since claims 2, 3, 4, 5, 6, 7, 10 and 11 after the amendment depend from claim 1, the invention as set forth in those claims has the novelty, the inventive step and the industrial applicability.

6. List of Annexed Documents

(Translation of the Second Amendment filed on 12.07.00)

WRITTEN AMENDMENT

(Amendment under the provision of Patent Law Section)

To: Commissioner of the Patent Office

1. Indication of International Application:

PCT/JP99/01350

2. Patent Applicant

Name: YASUKURA Yutaka

Mail Address: 15-22, Katsutadai-minami 2-chome,
Yachiyo-shi, Chiba-ken, 276-002 JAPAN

Nationality: Japan

Adress: Japan

3. Agent

Name: SEKI Masaharu, Patent Attorney (10434)

Mail Address: Seki Patent Office
Saiwai bldg. 4 Fl.
4, Gobancho, Chiyoda-ku, Tokyo 102-0076
Japan

4. Items to be Amended: Specification and Claims

5. Contents of the Amendment:

(1) In the specification, page 2, lines 17-26 (note: page

4, line 11 to page 5, line 6 in the English text), "A security assurance method ··· information file." is amended to "A security assurance method for electronic information of the present invention is characterized in that an electronic information file is divided into a plurality of information elements, and the divided information elements are selected and combined with their order changed to produce one or more information blocks. The information blocks are produced such that, if all of the information blocks are not integrated, then all of the information elements are not included. Further, division extraction data in which division information of the information elements and formation information of the information blocks are recorded is produced, and part of the information blocks and the division extraction data is transmitted to and stored into a certification station. Meanwhile, the other parts are stored or transmitted separately. Then, when the genuineness of the electronic information is to be confirmed, all of the information blocks and the division extraction data including the part stored in the certification station are collected and the information blocks are re-divided into the original information elements, re-arranged in the correct order and integrated based on the division extraction

data to restore the original electronic information file.

According to the security assurance method for electronic information of the present invention, part of information is deposited to the certification station and, when the original information is required, the information block in hand and the information block owned by the other party as well as the information block deposited to the certification station are joined to restore the information. Accordingly, even if one of the parties concerned and the certification station alters its information, the fact of the alteration is found clearly, and since the information stored by the certification station is not the entire information but part of the information, the information capacity required for the certification station may be small. Further, since the function of authenticating the security of information is divided into the three parties, it is an advantage in administration of the certification station that the burden on the certification station is light."

(2) In the specification, page 6, line 18 to page 7, line 2 (note: page 13, line 22 to page 15, line 4 in the English text), delete "Further, also where ··· station is light."

(3) In Claim 1, amend "to produce two or more information blocks in which all of the information elements are included if all of the information blocks are integrated" to "to produce two or more information blocks such that, if all of the information blocks are not integrated, then all of the information elements are not included", and amend "said information blocks and the division extraction data are stored or transmitted separately so that all of the information may not gather at a time; and when said electronic information is to be utilized, all of said information blocks and the division extraction data are collected" to "said information blocks and the division extraction data are separated so that all of the information may not gather at a time; at least one of said information blocks and the division extraction data separated is transmitted to and stored into a certification station while the others are stored or transmitted separately; and when the genuineness of said electronic information is to be confirmed, all of the information blocks and the division extraction data including that stored in the certification station are collected".

(4) In Claim 4, amend "are stored into an external storage apparatus to keep the electronic information in

said external storage apparatus in security." to "are stored into an external storage apparatus, and said external storage apparatus is disconnected from the system to keep the electronic information in security therein."

(5) In Claim 7, amend "an information element selected" to "one or more index information elements selected", and amend "the identity of said information elements" to "the identity of the index information elements".

(6) In Claim 10, amend "claims 5 to 9" to "claims 5 to 7".

(7) Delete claims 8, 9, 12 and 13.

6. List of the Annexed Documents

Specification page 2, page 2/1 (note: page 4, page 5, page 5/1 in the English text)

Claims page 19, page 20 (note: page 44, page 45, page 46, page 47 in the English text)

to provide a technique of assuring the security of electronic information by working electronic information to be stored or transmitted so that, even if the electronic information stored or being transmitted is stolen, it cannot be utilized thereby to decrease the value of the information and to provide a method of assuring the genuineness of information which a user has extracted or received to restore.

Disclosure of the Invention

A security assurance method for electronic information of the present invention is characterized in that an electronic information file is divided into a plurality of information elements, and the divided information elements are selected and combined with their order changed to produce one or more information blocks. The information blocks are produced such that, if all of the information blocks are not integrated, then all of the information elements are not included. Further, division extraction data in which division information of the information elements and formation information of the information blocks are recorded is produced, and part of the information blocks and the division extraction data is transmitted to and stored into a certification station.

Meanwhile, the other parts are stored or transmitted separately. Then, when the genuineness of the electronic information is to be confirmed, all of the information blocks and the division extraction data including the part stored in the certification station are collected and the information blocks are re-divided into the original information elements, re-arranged in the correct order and integrated based on the division extraction data to restore the original electronic information file.

According to the security assurance method for electronic information of the present invention, part of information is deposited to the certification station and, when the original information is required, the information block in hand and the information block owned by the other party as well as the information block deposited to the certification station are joined to restore the information. Accordingly, even if one of the parties concerned and the certification station alters its information, the fact of the alteration is found clearly, and since the information stored by the certification station is not the entire information but part of the information, the information capacity required for the certification station may be small. Further, since the function of authenticating the

security of information is divided into the three parties, it is an advantage in administration of the certification station that the burden on the certification station is light.

It is to be noted that the division extraction data may be stored or transmitted separately, and the division extraction data relating to the information elements may be produced and annexed for each of the information elements.

Claims:

1. (As amended) A security assurance method for electronic information, characterized in that an electronic information file is divided into a plurality of information elements; the divided information elements are selected and combined with their order changed to produce two or more information blocks such that, if all of the information blocks are not integrated, then all of the information elements are not included; division extraction data in which division information of said information elements and formation information of the information blocks are recorded is produced; said information blocks and the division extraction data are separated so that all of the information may not gather at a time; at least one of said information blocks and the division extraction data separated is transmitted to and stored into a certification station while the others are stored or transmitted separately; and when the genuineness of said electronic information is to be confirmed, all of the information blocks and the division extraction data including that stored in the certification station are collected and said information blocks are re-divided into the original information elements, re-arranged in the correct order and integrated

based on said division extraction data to restore the original electronic information file.

2. A security assurance method for electronic information according to claim 1, characterized in that said division extraction data is stored or transmitted separately by different means from that with which said information blocks are stored or transmitted.

3. A security assurance method for electronic information according to claim 1, characterized in that said division extraction data relating to said information elements is annexed for each of said information elements.

4. (As amended) A security assurance method for electronic information according to any one of claims 1 to 3, characterized in that said information blocks and the division extraction data are stored into an external storage apparatus, and said external storage apparatus is disconnected from the system to keep the electronic information in security therein.

5. A security assurance method for electronic information according to any one of claims 1 to 3, characterized in that a plurality of said information blocks are formed, and said blocks are transmitted in a separate state from each other to a recipient together with said division extraction data.

6. A security assurance method for electronic information according to claim 5, characterized in that said division extraction data includes data for confirmation of the originality of said electronic information file.

7. (As amended) A security assurance method for electronic information according to any one of claims 1 to 6, characterized in that one or more index information elements selected from among said information elements is included commonly into a plurality of information blocks, and when the information elements are integrated, the identity of the index information elements included commonly in an overlapping relationship in the different information blocks is verified to confirm the security of the information.

8. (Deleted).

9. (Deleted).

10. (As amended) A security assurance method for electronic information according to any one of claims 5 to 7, characterized in that at least one of said information blocks and said division extraction data is transmitted to the recipient by second transmission means different from the transmission means for the other electronic information.

11. A security assurance method for electronic

information according to claim 10, characterized in that a transfer station is interposed in said transmission means or said second transmission means, and a block of the information to be sent by said transmission means is accommodated into an information package together with destination information and sent to said transfer station, which in turn transfers the information block to said recipient based on said destination information.

12. (Deleted).

13. (Deleted).

世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G09C 1/04, 1/00, H04L 9/32	A1	(11) 国際公開番号	WO00/45358
		(43) 国際公開日	2000年8月3日(03.08.00)

(21) 国際出願番号 PCT/JP99/01350

(22) 国際出願日 1999年3月18日(18.03.99)

(30) 優先権データ
特願平11/19399 1999年1月28日(28.01.99) JP

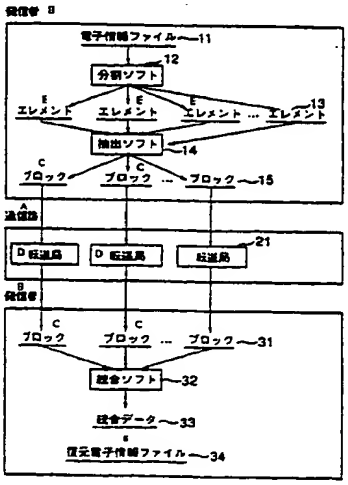
(71) 出願人；および
(72) 発明者
保倉 豊(YASUKURA, Yutaka)[JP/JP]
〒276-0025 千葉県八千代市勝田台南二丁目15番22号
Chiba, (JP)
(74) 代理人
関 正治(SEKI, Masaharu)
〒102-0076 東京都千代田区五番町4番地 幸ビル4階
関特許事務所 Tokyo, (JP)

(81) 指定国 AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), ARIPO特許 (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM)

添付公開書類
国際調査報告書

(54)Title: METHOD FOR SECURING SAFETY OF ELECTRONIC INFORMATION

(54)発明の名称 電子情報の安全確保方法



11...ELECTRONIC INFORMATION FILE
12...DIVIDING SOFTWARE
E, 13...ELEMENT
14...EXTRACTING SOFTWARE
C, 15, 31...BLOCK
D, 21...TRANSFERT STATION
32...INTEGRATED SOFTWARE
33...INTEGRATED DATA
34...RESTORED ELECTRONIC INFORMATION FILE
A...COMMUNICATION CHANNEL
B...SENDER

(57) Abstract

A method for securing safety of electronic information, in which an electronic information file (1) is divided into information elements (2), the information elements are combined in a different order to produce one or more information blocks (3), information element division/extraction data is generated to produce an information block and store or transmit it, the information blocks (3) are divided into information elements (4) again based on the division/extraction data when the electronic information is used, the information elements (4) are arranged in the correct order and integrated to restore the original electronic information file (5), thus resulting in diminishing the value of the information not to be used even if the electronic information stored or being transmitted is stolen.

(57)要約

電子情報ファイル１を複数の情報エレメント２に分割し、分割された情報エレメントを選択し順序を変えて組み合わせることにより１個以上の情報ブロック３を生成し情報エレメントの分割抽出データを生成して情報ブロックを形成して格納もしくは伝送し、電子情報を使用するときに分割抽出データに基づいて情報ブロック３内の情報エレメント４を再分割し、正しい順序に並べ直して統合することにより、元の電子情報ファイル５を復元するようにして、保管中や通信中の電子情報が窃取されることがあってもその情報価値を減殺して利用できないようにした電子情報の安全確保手法。

明細書

電子情報の安全確保方法

技術分野

この発明は、電子情報の保管あるいは電子情報の交換における電子情報の安全確保方法に関し、また電子情報の原本との同一性を保証する方法に関する。

背景技術

多数のコンピュータが通信網に接続されてシステムを形成するようになって、各コンピュータが通信路を介して不特定多数の人と連結されうるようになってきた。このため、ハードディスク装置などコンピュータの外部記憶装置に格納した電子情報も通信路を介して権原のない他人にアクセスされて盗用や改竄をされる心配がある。

また、電子メールその他の個人情報交換、ゲームプログラムやビジネスプログラムなどのアプリケーションプログラムの配布、データベースから抽出編集されたデータの配布など、電子情報を通信路を用いて伝送することが多くなってきた。このような電子情報交換に外部に解放された通信環境を使用する場合には、傍受あるいは窃盗行為などにより受信者でない他人が通信中の電子情報を入手して利用する可能性がある。特に有料で情報を配布する場合やプライバシーに係わる情報を伝送する場合には、通信中の電子情報を容易に盗用されないようにする必要がある。

無関係の他人が電子情報を入手しても利用できなくするため、暗号化することにより電子情報の秘密性を確保する方法が行われている。このような目的に開発された暗号化技術は、対称鍵を用いた暗号方式、非対称鍵を用いた暗号方式、それぞれ多様に存在する。

しかし、これら暗号化技術を用いても、保管されている電子情報や伝送されている電子情報には全ての情報が含まれているため、暗号の解読など何らかの手段で復号方法を入手した者があれば、容易に復元して有用な情報を入手することができる。また、情報の改竄や偽造も可能で、取り出したり受け取った電子情報が

真正な情報を維持しているか否かを常に心配しなければならない。特に本人認証データなど、高い秘匿性が要求される電子情報を保管したり伝送する場合に、従来方法では不安がある。

保管中や通信中に改変を受けたり情報の欠落があった場合には、取出しあるいは受信した情報の多くは正しい利用ができなくなり、また正しくない情報をそのまま使用して不都合を招来する場合もある。また、情報が第三者に知られること自体が問題となる場合がある。したがって受信した電子情報が送り出したものとの同一性を保持していることを確認するため、また電子情報が正当に使用されることを確認するための便利な手法が要求される。

そこで、本発明は、保管や伝送をしようとする電子情報を加工して、たとえ保管中や通信中の電子情報が窃取されることがあっても利用できないようにして情報価値を減殺することにより電子情報の安全を確保する手法を提供することを目的とし、また使用者が取り出しあるいは受信して復元しようとする情報の真正性を保証する方法を提供することを目的とする。

発明の開示

本発明の電子情報の安全確保方法は、電子情報ファイルを複数の情報エレメントに分割し、分割された情報エレメントを選択し順序を変えて組み合わせることにより１個以上の情報ブロックを生成する。この情報ブロックは、全ての情報ブロックを統合すると全ての情報エレメントが含まれるようにする。さらに情報エレメントへの分割方法と情報ブロックの形成方法を記録した分割抽出データを生成し、情報ブロックおよび分割抽出データを保管もしくは伝送する。そして、電子情報を使用するときに、すべての情報ブロックと分割抽出データを集合し、分割抽出データに基づいて情報ブロック内の情報エレメントを再分割し、正しい順序に並べ直して統合することにより、元の電子情報ファイルを復元することを特徴とする。

なお、分割抽出データを別途に格納もしくは送付するようにしてもよく、また、各情報エレメントに係る分割抽出データを生成して情報エレメント毎に付帯させてもよい。

本発明の電子情報の安全確保方法によれば、保管あるいは送付すべき電子情報ファイルを適当な数の適当な長さの情報エレメントに分割した上でシャッフルして組み合わせることにより１個以上の情報ブロックを形成し、この情報ブロックを外部記憶装置に格納しあるいは受信者に送付する。

したがって、保管中あるいは通信中の電子情報はシュレッダにかけられた紙情報と同様に復元しない限り役に立たない状態になっているので、復元手段を持たない他人がアクセスしても価値を有する情報として漏洩する訳ではなく安全である。

電子情報ファイルに対して１個の情報ブロックしか形成しない場合でも、情報ブロック内に収納された情報エレメントの順序が入れ替わっているため情報を判読することが困難である。しかし、複数の情報ブロックを形成してそれぞれを別々に保管あるいは送付するようにすれば、たとえ他人が一部の情報ブロックを盗窃しても電子情報の全容が盗まれることにはならないので、より安全性が向上することはいうまでもない。

また、情報ブロックはさらに暗号技術を適用して保管あるいは送付するようにして、格段の安全性向上を図ることもできる。

分割抽出データは、情報ブロックを形成するときに用いられた分割・組合わせに必要なデータであって、情報ブロックと共に格納あるいは送付する。分割抽出データは情報エレメント毎の電子情報ファイルにおける位置情報や長さ情報を含むものであるから、情報エレメント毎に付帯させておいて情報ブロックと一緒に扱っても良い。また、安全性を重視する場合には情報ブロックとは別途に扱うようにしても良い。

電子情報を取り出す者や受信する者は全部の情報ブロックを集め、分割抽出データを使用して、各情報ブロックに含まれる情報エレメントをそれぞれに分離し、正しい順に再結合して元の電子情報に復元する。

コンピュータの外部記憶装置に電子情報を記憶させるときに、電子情報ファイルを上記のように処理して情報ブロックと分割抽出データを生成して、これらを外部記憶装置に記憶させるようにしてもよい。

本発明の安全確保方法を記憶装置に適用することにより、他人のアクセスがあ

っても価値ある情報の流出には結びつかず、コンピュータにおける電子情報保管の安全性が向上する。

なお、電子情報を送付するときには、電子情報ファイルを複数の情報エレメントに分割し、分割された情報エレメントを選択し組み合わせて複数の情報ブロックを形成して、情報ブロックのそれぞれを分離した状態で受信者に伝送すると共に分割抽出データを受信者に伝送し、これらのデータを受け取った受信者側で分割抽出データに基づいて情報ブロックに含まれる情報エレメントを再分割し正しい順に統合して元の電子情報に復元するようにすることが好ましい。

電子情報ファイルを送付するときは使用する通信路が広く一般に解放されていることがあるため、より高度な安全性を有することが好ましい。このような場合にも、複数の情報ブロックを異なる通信手段で送付するようにすることにより格段に高い安全を確保することができる。

本発明における情報ブロックはそれぞれ必要な情報の一部を搭載しているだけなので、たとえ通信途中で一部の情報ブロックを入手しても情報の全体を復元することはできない。

したがって、情報ブロックおよび分割抽出データのうち少なくとも1個を他の電子情報の伝送手段と異なる第2の伝送手段により受信者に送付するようにすることが好ましい。

情報ブロックおよび分割抽出データを全て同じ伝送手段を用いて送付しないで、そのうちのいくつかを異なる伝送手段により送付する場合は、通信路途中に窃取者が存在しても全部の情報を集めることができないので、より安全である。

情報ブロックをそれぞれ異なる時刻に送ったり、別の通信ルートを使用して送るようにすれば、通信路の途中で全ての情報ブロックを漏らさず窃取することは非常に困難であり、せいぜい情報の一部を入手できるだけであるから、たとえば本人認証データを送付する場合にも、他人がこれを盗用することを避けることができる。

なお、分割抽出データには電子情報ファイルの原本性を確認するデータを含ませることが好ましい。送付しようとした電子情報ファイルと受信者が復元した電子情報が同一のものであることは、分割抽出データと受け取った情報ブロックの

内容が矛盾していないことを検証することにより高い確度で確認することができる。

また、送付しようとした電子情報ファイルと受信者が復元した電子情報が同一のものであることは、別の通信ルートで送付される情報ブロックに情報エレメントの内から選択した情報エレメント、すなわちキーエレメントが共通して含まれるようにして、情報エレメントを統合するときに受信した情報ブロックに重複して含まれているキーエレメント同士の同一性を検証することにより確認するようにしてもよい。

なお、送付された電子情報ファイルが送付しようとした電子情報ファイルと同じ物であることを確認するためには、それぞれのファイルに含まれる語数が一致しているか否かを調べるという簡単な方法もある。

本発明の電子情報の安全確保方法をアプリケーションプログラムやデータベースのオンライン販売に用いれば、正当な購買者以外の者が通信中の電子情報を窃取しても一部の情報しか入手できないので、プログラムを実行することができず、また有用な情報を取得することができない。したがって通信中の電子情報を窃取する動機がないため、販売者の利益が窃取により損なわれることがない。

また、本人認証データを送付するために適用すれば、他人の盗用や偽造を確実に防止して、安全性の高い情報交換ができる。

さらに厳格な保証が必要なときには、送付する電子情報の原本を保存し、受信者側で復元した電子情報を返送させ、電子情報原本と照合して同一性を確認するようにすることが好ましい。

さらに、受信者が復元した電子情報を返送させ、保存してある電子情報原本と照合して同一性を確認するようにすれば、通信の途中で改竄されたり通信情報の一部が欠落したりした場合にも直ちに判定して対策をとることができる。

なお、受信者が入手した情報ブロックをそのまま返送させて電子情報原本と照合するようにしてもよい。情報ブロック毎に検査することにより障害を受けた部位を特定することができ、対策が容易になる。

原本と差異がある場合は、通信路の信頼性を疑って再度情報を送付したり、改竄者の介入を回避して通信路を変更したりすることができる。なお、受信者も送

信者からの照合結果を受け取ることにより安心して電子情報を利用することができる。

伝送手段中に中立的で公正な転送局を配設し、転送局を介して情報伝送を行うようにすると信頼性が向上する。転送局は自局宛に送られた情報パッケージに含まれる情報ブロックを宛先情報に基づいて受信者に転送する。

このようなルートを使用して情報ブロックを送付する場合は、分割された情報ブロックの外見がそれぞれ異なるため、通信路途中の窃取者が電子情報ファイルを復元するために必要となる情報ブロックを全て収集することが困難になり、安全性はさらに向上する。

特に、分割抽出データを含む部分を転送局を介して送付するようにしただけでも、システム全体の信頼性が向上する。

なお、転送局が暗号技術を適用して電子情報を転送するようにすれば、より高度な安全性を確保することができる。

また、送信された情報は必ずしも受信者が直ちに使用するとは限らない。そこで送信者が送付した情報ブロックを転送局で保管しておいて、受信者が必要に応じて転送局に情報ブロックを送信させ、収集した情報ブロックを統合し復元して利用するようにしても良い。

さらに、当事者間の争いを避けるため証明局を介在させて電子情報の同一性を保証するシステムを利用する場合にも、電子情報ファイルを分割して得られる情報ブロックを証明局と当事者がそれぞれ分かち持つようにして、電子情報を使用するときに証明局と当事者とから関連する情報ブロックを収集し統合して元の電子情報に復元するようにして、電子情報の安全性を保証するようにすることができる。

この方法では、本発明の電子情報の安全確保方法を利用し、情報の一部を証明局に預けておいて元の情報を必要とするときに手元の情報ブロックと相手の所有する情報ブロックに加えて証明局に預けた情報ブロックを合わせて復元するようにする。したがって、当事者と証明局のいずれが情報を改竄しても改竄の事実が明確に分かる上、証明局が保管するのは情報全体でなく一部であるので、証明局の備えるべき情報容量は小さくて良い。また、情報の安全性を認証する機能が三

者に分割されているため証明局としての負担も少ないことが証明局運営上の利点となる。

図面の簡単な説明

第１図は本発明の電子情報の安全確保方法の概念を説明するブロック図、第２図は本発明の１作用を説明する図面、第３図は本発明の電子情報の安全確保方法に係る第１実施例を表すフローダイヤグラム、第４図は本実施例を使用したシステムのブロック図、第５図は本発明の電子情報の安全確保方法に係る第２実施例を表すフローダイヤグラム、第６図は本実施例を使用したシステムのブロック図、第７図は本発明の電子情報の安全確保方法に係る第３実施例を表すフローダイヤグラム、第８図は本実施例を使用したシステムのブロック図、第９図は本発明の電子情報の安全確保方法に係る第４実施例を表すフローダイヤグラム、第１０図は本発明の電子情報の安全確保方法に係る第５実施例を表すブロック図、第１１図は本発明を適用した証明局の機能を説明するブロック図である。

発明を実施するための最良の形態

本発明の電子情報の安全確保方法は、電子情報ファイルの保管あるいは通信において電子情報の安全を確実にする方法である。本発明の方法により、保管中や通信途中で電子情報を窃取する者があっても窃取によって入手できる情報の有する価値を小さくして窃盗の被害を防ぐと共に、窃盗の利益を減殺したことにより窃取行為を予防し、また通信中に情報の欠落や情報の改竄があったときにはその事実を検知するようにして安全性を確保する。

以下、図面を参照して本発明の詳細を説明する。

第１図は本発明の概念を説明するブロック図、第２図は発明の１作用を説明する図面である。第１図は、本発明の使用態様の１例として、電子情報ファイルを６個の情報エレメントに分割し２個の情報ブロックに分けた場合を示している。

本発明の電子情報の安全確保方法では、対象とする電子情報ファイル１を適当な数の情報エレメント２に分割する。ここでは、簡単のため、６個の情報エレメントＡ，Ｂ，Ｃ，Ｄ，Ｅ，Ｆに分割する場合を例として説明している。情報エレ

メント２は情報として意味がある位置で区切る必要はなく、盗用される可能性を少なくするためには、電子情報ファイル１を単に物理的に分割したものである方が好ましい。

分割した情報エレメントＡ，Ｂ，Ｃ，Ｄ，Ｅ，Ｆの配列順を変更し適当にグループ化して適当数の情報ブロック３を形成する。

図示した例では、第１の情報ブロック３に情報エレメントＡ，Ｄ，Ｅを配分し、第２の情報ブロック３に情報エレメントＢ，Ｃ，Ｆを配分している。なお、情報ブロック３内の情報エレメントの配列順も任意に変更することができる。

このような情報ブロック３を他人が読み出しても、情報エレメントＡ，Ｂ，Ｃ，．．．が意味のある配列になっていないため、そのままでは電子情報の内容を読みとることができない。

また、電子情報が分割されているため、全ての情報ブロックを入手しないと内容を復元できない。たとえば第２図（ａ）に示す本人認証データを第２図（ｂ）に示すように分割したときには、一方の情報ブロックを入手して復元に成功しても、認証データとして利用することができない。このため不正にアクセスする者がいても電子情報を利用できるようにすることは容易でなく、情報の安全を保持することができる。

この情報ブロック３を目的に応じて記憶装置に保管し、あるいは受信者に送付する。

電子情報の使用者は保管先から取得したり送信者から受信した情報ブロック３を元の情報エレメント４（Ａ，Ｂ，Ｃ，．．．）に分割し、これらを正しい順序に並べ直して使用可能な電子情報ファイル５に戻すことにより元の電子情報ファイル１を復元する。

電子情報ファイル１を復元するために必要となる基礎的な情報は、各ブロック３に含まれる情報エレメントＡ，Ｂ，Ｃ，．．．の区切り情報と、各情報エレメントの電子情報ファイル１における位置と長さの情報である。

目的の電子情報ファイル１に関連する情報ブロック３を全て収集した上で、情報ブロック３内の情報エレメントを切り出し、各情報エレメント２の先頭番地と語長の情報を用いて、正しい順に並べ直すことができる。

また、電子情報ファイル１を復元するときに、目的の電子情報ファイル１を特定する情報や、情報エレメント２を並べ替えて情報ブロック３を形成したときの各ブロックに含まれる情報エレメントの配列順序の情報を利用してもよい。

電子情報ファイル１を復元するときには、まず、集めた情報ブロック３が目的の電子情報ファイル１に関連するものであり、関連する全ての情報ブロックが落ちなく集まっていることを確認する必要がある。このとき、情報ブロックや情報エレメントに識別領域Ｘ１，Ｘ２を付帯させ、この識別領域に電子情報ファイル１を特定するＩＤ情報を記載して利用すると効率よく作業ができる。

また、区切り情報を用いて各ブロックに含まれる情報エレメントを再分割し、さらに分割された情報エレメント４の配列順にしたがって再配列して得た電子情報ファイル５は元の電子情報ファイル１と同じ物となる。

なお、復元した電子情報ファイル５と元の電子情報ファイル１が同じ物であるか否かは、たとえば両者の総語長を比較することで、ある程度の確度をもって検証することができる。

これらの基礎的情報を含む分割抽出データは、情報ブロック３を形成するときに作成されて、情報ブロック３の一部に識別領域を添付して格納あるいは送付され、電子情報ファイル１を復元するために利用される。分割抽出データは、情報エレメント毎に添付するようにしてもよい。

なお、分割抽出データは情報ブロック３とは別途独立に保管あるいは送付されるようにしても良い。

本発明の電子情報の安全確保方法では、１個の電子情報ファイル１に対応する情報ブロック３は２個に限らず、３個以上の複数でもよく、また１個であっても良い。いずれも情報ブロック３内の情報エレメントの配列が元のものと異なるため他人が読み出して利用することができないので電子情報の安全を保持することができる。

（実施例１）

第１の実施例は、本発明の電子情報の安全確保方法を適用して、電子情報ファイルを通信路を使用して安全に相手方に送信するものである。

第３図は本実施例を表すフローダイアグラム、第４図は本実施例を使用するシ

ステムのブロック図である。

まず、第３図と第４図を参照して本実施例の基本的な態様について説明する。

電子情報の発信者は、まず送信しようとする電子情報に関係して、新たに作成したりデータベースから抽出して編集することにより、電子情報ファイル１１を準備する（Ｓ１）。対象になる電子情報の例として、本人認証データのような高度の安全性を要求されるようなものや、通信路を介して販売されるソフトウエアなど有価のものなどがある。

次に、分割ソフト１２を用いて電子情報ファイル１１を複数の情報エレメント１３に分割する（Ｓ１２）。分割ソフト１２には情報エレメント１３のおのおのに関して電子情報ファイル１１内の分割位置と情報エレメントの語長を指示できるようになっている。

なお、分割位置と語長を各情報エレメント毎に指示する代わりに、分割数を指定すると分割ソフト１２が自身で決定するようにしても良い。分割数は任意に決めることができるが、１００kByte程度までの電子情報を対象にするときにはたとえば１００以内の個数を選択するように決めてもよい。

次に、抽出ソフト１４を用いて情報エレメント１３を複数の情報ブロック１５に配分する（Ｓ３）。抽出ソフト１４は、分割された情報エレメント１３の順番を入れ替えて再配列する機能と、これらを情報ブロック１５に分配する機能を有する。情報ブロック数はオペレータが指示できるようになっている。

また、情報エレメント１３の分割情報および再配列の結果は分割抽出データとして電子情報化し、それぞれ情報エレメント１３に付帯させる。各情報ブロック１５に配分された全ての情報エレメント１３の分割抽出データをまとめて情報ブロック１５の識別領域Ｘ１，Ｘ２に付帯させても良い（Ｓ４）。

なお、識別領域Ｘ１，Ｘ２には、発信者や受信者に関するデータ、制作者や所属など電子情報に関するデータ、利用者や有効期限など電子情報を利用できる範囲を記述したデータ、統合ソフトなど適用するソフトを特定するデータなどを付帯させてもよい。

また、識別領域に電子情報を指示するＩＤを記述しておくと情報ブロックの仕訳が容易になるので、受信者が再統合して電子情報ファイルを復元するために目

的の電子情報に係わる情報ブロックを収集する場合に便利である。

なお、分割抽出データは情報ブロックとは別途独立に受信者に送付するようにしても良い。また、各情報ブロックに分散して付帯させる代わりに、いずれかの情報ブロックにまとめて付帯させても良い。さらには全ての情報ブロックに電子情報ファイル全体に関する分割抽出データを付帯させるようにしても良い。

次に、各情報ブロック１５をそれぞれ転送局２１に送信するためのパッケージに収納する（Ｓ５）。パッケージには最終的に受信するべき者の宛名を収納しておく。このパッケージを暗号処理して転送局２１に送る（Ｓ６）。暗号処理は適当な公知方法を適用して行えばよい。

このとき、パッケージ毎に異なる送り先を選ぶことができる。通信路の危険性や電子情報の性格から決まる安全性の程度に基づいて、使用する通信手段を選択する。漏洩や改竄を極端に嫌う場合はできるだけ多数の通信手段を使用するようにする。

なお、情報漏れの危険が小さいときには転送局が存在しない通常の通信路を使用しても良い。本発明の安全確保方法は、電子情報を分割して再配列した状態で通信路に置くため高い安全性を有するので、通常の通信路を使用しても従来方法と比較して十分安全である。

また、通信手段として、例えば郵便を用いてフロッピーディスクなど可搬の記憶装置を送る方法などを選択することもできる。

パッケージを受け取った転送局２１は、これを復号化して収納された宛先情報を読みとる（Ｓ７）。

次に、パッケージに収納された情報ブロックを再度暗号化して指示された受信者に向けて送付する（Ｓ８）。

このように情報ブロック１５が外見から内容が分からない状態になって別々の転送局に配送されるため、他人が通信路中に存在する電子情報を入手できたとしても、必要な情報を判別して収集することが困難で目的の電子情報を復元することができない。

受信者は転送局から送り込まれた情報ブロック３１を受信して（Ｓ９）復号し、情報ブロックもしくは情報エレメントの識別領域部分をサーチすることにより、

目的の電子情報を復元するために必要となる情報ブロック３１を全て収集する（Ｓ１０）。

また、識別領域部分の分割抽出データから情報エレメント１３を生成したときの分割情報と情報ブロック１５を生成したときの抽出情報を取り出す（Ｓ１１）。

次いで、統合ソフト３２を用いて、分割情報と抽出情報に基づいて情報ブロック３１を再分割し元の情報エレメント１３を切り出し（Ｓ１２）、元の順序に配列し直す（Ｓ１３）。

最後に、全部の情報エレメントを合体し統合して電子情報ファイル３３を形成する。このとき、統合して形成された電子情報ファイル３３の全長を分割抽出データに含まれている元ファイルの全長値と比較する（Ｓ１４）。両者が一致すれば、かなり高い確度で元の電子情報ファイル１１が復元できたとすることができる。さらに、原本の性格を記述する情報や適当なしおりを挿入した位置情報などを用いて原本との同一性をより正確に確認するようにすることも可能である。

（実施例２）

第２の実施例は本発明の電子情報安全確保方法において、さらに高度に電子情報の原本性を保証する手段を備えたものである。

第５図は電子情報の発信者において原本性を確認する手段を備えた第２実施例の電子情報安全確保方法を表すフローダイアグラム、第６図はそのブロック図である。

以下、第５図と第６図により、電子情報の発信者において原本性を確認する手段を備えた本発明の実施例を説明する。

なお、本実施例において基本となる安全確保方法については、既に説明したものと同じであるので、以下ではその部分を簡約したり省略することにより誤解を招かない程度に説明の重複を避けることにする。

発信者は送付すべき電子情報ファイル１１を生成したときに、その原本から写本１７を生成し（Ｓ２１）、写本１７を保存する（Ｓ２２）。なお、写本１７の代わりに原本１１を保存しても同じである。

次に、分割抽出ソフト１６を用いて、既に説明した第１実施例と同じように、操作者から与えられた、あるいは一部コンピュータで生成した分割情報と抽出情

報に基づいて電子情報ファイルの原本１１を加工して情報ブロック１５を形成する（Ｓ２３）。なお、原本１１を保存する場合は加工する対象を写本１７にする。

情報ブロック１５はそれぞれ第１実施例と同じようにして転送局２１宛てに送付する（Ｓ２４）。

転送局２１は、受信した情報ブロック１５を指示された受信者に転送する（Ｓ２５）。

受信者は受信した情報ブロック３１を調べて、目的の電子情報を復元するために必要な情報ブロック３１を全て集める（Ｓ２６）。

次に、取得した分割抽出データに含まれる抽出情報と分割情報に基づき、統合ソフト３２を用いて、各情報ブロック３１内の情報エレメントを抽出し配列順を正して統合し電子情報ファイル３３を形成する（Ｓ２７）。

さらに、形成された電子情報ファイル３３の写本３５を生成し（Ｓ２８）、これを送信と同様の方法で転送局２２を介して電子情報の発信者に返送する（Ｓ２９）。この場合の転送局２２は、送信の場合と同様に複数であることが好ましい。また、返送する電子情報ファイルの写本３５は暗号化処理を施して安全性を高めておくことが好ましい。

発信者は、受け取った復元電子情報ファイルの写本３５と保存しておいた電子情報ファイル写本１７とを比較照合して、同一性を確認する（Ｓ３０）。

両者が一致しない場合は電子情報として使用できないので受信者にその旨を通知する（Ｓ３１）。受信者は発信者からの警報通知を受けない場合は情報ファイルの復元が正常に行われたと判断することができる（Ｓ３２）。

なお、二つのファイルが一致しない場合は、通信中に何らかの障害があったことを示すので、原因を究明して排除し次回以降の通信を安全に行えるようにしなければならない。原因の排除ができない場合は通信手段を変更することが好ましい。

このようにして、受信者における電子情報の復元が正しく行われたことを発信者が確認するようにすることにより、極めて信頼性の高い電子情報交換が実現することになる。

（実施例３）

第３の実施例は、本発明の電子情報の安全確保方法において、情報ブロック毎に原本性を確認する手段を備えて、個々の通信路の異常を検出して対策をより容易にする電子情報の原本性保証方法である。

第７図は本実施例を表すフローダイアグラム、第８図は本実施例を使用するシステムのブロック図である。以下、第７図と第８図により、本実施例を詳細に説明する。

なお、本実施例についても、既に説明したものと同じ部分を簡約したり省略することにより説明の重複を避けることにする。

発信者は、第１実施例におけると同様に、送付すべき電子情報ファイル１１を作成し（Ｓ４１）、分割情報と抽出情報に基づいて情報エレメントを切り出しこれをシャッフルして情報ブロック１５を形成する（Ｓ４２）。

情報ブロック１５から写本を生成して保存しておく（Ｓ４３）。

次に、第１実施例と同じ方法で転送局２１に情報ブロック１５を収納したパッケージを送付すると（Ｓ４４）、転送局２１はパッケージを復号して受信者の宛名を読みとり情報ブロック１５を改めて指定された受信者に転送する（Ｓ４５）。

受信者は受け取った情報ブロック３１の写本を作成して（Ｓ４６）、転送局２３を介して発信者に返送する（Ｓ４７）。

発信者は、返送された情報ブロック３１の写本と保存してある元の情報ブロック１５の写本とを照合して一致するか否かを確認する（Ｓ４８）。

両者が一致するときは通信中に変成を受けなかったのでそのまま使用して電子情報の復元ができる。

また、両者が一致しないときには、その情報ブロックを伝達した通信路に異常があることを示す。上記第２の実施例においては、異常の検出は可能であるが、全ての通信路を統合した形で検出するので、異常のある通信経路を特定することが困難であった。しかし、本実施例における方法を使用すると上記の通り簡単に異常経路を特定することができる。したがってまた、障害の除去などの対策が容易である。

発信者が行った照合の結果は受信者に通知される（Ｓ４９）。

照合の結果、２つの写本が一致するときは統合ソフト３２を用いて第１実施例

と同じ手順で電子情報ファイルの復元を行う（Ｓ５０）。情報ブロック３１から形成された統合データ３３は元の電子情報ファイル１１と同じ内容を持つファイル３４になる。

なお、電子情報の交換は上記のような転送局２１，２３が存在しない通信路を用いて行っても良いことは第１実施例の説明において述べたとおりである。

また、転送局は送信者が送付した情報ブロックを保管しておいて、受信者の要求に従ってその情報ブロックを送信するようにしてもよい。受信者は全部の情報ブロックを収集し、これらを統合し復元して利用する。

（実施例４）

第４の実施例は本発明の電子情報の安全確保方法を適用して、電子情報ファイルをコンピュータシステムの外部記憶装置に保管するものである。

第９図は本実施例の電子情報安全確保方法を使用するコンピュータシステムのブロック図である。

以下、図面を参照して本実施例について説明する。

なお、本実施例における構成要素の作用効果は、上記説明した各実施例におけるものと共通する部分が多いので、上記実施例と同じ機能を備える構成要素部分については同じ参照番号を付し説明を簡約にし、重複を避けている。

コンピュータシステムで作成した電子情報ファイル４１は、分割抽出ソフト４２により情報エレメントに分割して再配列し、複数の情報ブロック４３に配分してから記憶装置５０に格納される。

記憶装置５０から取り出すときは、対象とする電子情報を担持している情報ブロック６１を全て収集し、統合ソフト６２を実行する。統合ソフト６２は情報ブロック６１から分割情報と抽出情報を抽出し、これら情報に基づいて情報ブロック６１内の情報エレメントを切り出し、元の順に配列し直して統合し、電子情報ファイル６３を生成する。

本実施例の電子情報安全確保方法を用いると、記憶装置５０に収納されている電子情報ファイルが複数の情報ブロックに分割されていて、目的の電子情報が復元できるように関係する情報ブロックを全て集めることは難しい。また、情報ブロック内部の情報エレメントもシュレッダにかけられた紙情報のようにバラバラ

になっているので、電子情報の一部を再現することも容易でない。

このようにして、外部からのアクセスにより情報が漏洩することを防止することができる。

なお、記憶装置５０に記録する際に暗号処理を施しても良い。

また、記憶装置５０は１個の記憶装置である必要はなく、情報ブロック毎に別個の記憶装置に保存するようにしても良い。

本実施例の電子情報安全確保方法は、機密性が特に要求される認証局において本人認証データをハードディスク装置や磁気テープ装置など外部記憶装置に保存するときに適用することができる。

（実施例５）

第５の実施例は本発明の電子情報の安全確保方法において、電子情報の一部を利用して電子情報の原本性を保証する手段を備えたものである。第１０図は、本実施例に用いた原本性保証手段を説明するブロック図である。本実施例において基本となる電子情報の安全確保方法については、既に説明したものと同じであるので、以下ではその部分を簡約して説明の重複を避けることにする。

第１０図は、本発明の使用態様の１例として、電子情報ファイルを７個の情報エレメントに分割し２個の情報ブロックに分けた場合を示している。

分割した情報エレメントＡ，Ｂ，Ｃ，Ｄ，Ｅ，Ｆ，Ｇは配列順を変更し適当にグループ化して２個の情報ブロックに配分される。このとき、情報エレメントの内のいくつかはキーエレメントとして両方の情報ブロックに共通して含まれるようにする。また、情報ブロックには情報エレメントの区切り情報と電子情報ファイルにおける位置と長さの情報と電子情報ファイルのＩＤ情報などを記録した識別領域Ｘ１，Ｘ２を付帯させて復元のために利用できるようにしておく。

第１０図に図示した例では左の情報ブロックに情報エレメントＡ，Ｂ，Ｃ，Ｅ，Ｆが配分され、右側の情報ブロックには情報エレメントＢ，Ｄ，Ｅ，Ｇが配分されていて、情報エレメントＢとＥがキーエレメントとしていずれの情報ブロックにも含まれている。各情報ブロック中の情報エレメントは適当に順位が入れ替わっていて意味のある配列になっていないため、情報ブロックを他人が読み出してもそのままでは電子情報の内容を読みとることができない。この情報ブロックは

目的に応じて記憶装置に保管され、あるいは受信者に送付される。

電子情報の使用者は入手した情報ブロックを、識別領域Ｘ１，Ｘ２に記録された情報に基づいて、元の情報エレメント（Ａ，Ｂ，Ｃ，．．．）に分割しこれらを正しい順序に並べ直して元の電子情報ファイルを復元する。

復元時には、２つの情報ブロックに重複して含まれキーエレメントとなっている情報エレメントＢ，Ｅを検出して照合する。すると、いずれかの情報ブロックが情報の保管時あるいは伝送時に何らかの改変を受けたときには、重複する情報エレメントの内容が一致しないので簡単に異常の検知ができる。

本実施例に用いた異常検出方法は、情報ブロックを単独に観察しても照合対象とするキーエレメントを抽出することができないので容易に第三者の攻撃を回避することができる。また、特別な付加情報を必要とせず安全性を確認するための情報処理が簡単である。

なお、本実施例の異常検出方法を他の方法と併用して安全性を向上させても良いことは言うまでもない。

（実施例６）

第６の実施例は本発明の電子情報の安全確保方法を適用して、各所に電子情報を分割して保管し、当事者間の取引内容などの照合証明を正確に行う証明局に関するものである。

第１１図は本発明を適用した証明局の機能を説明するブロック図である。本実施例において基本となる安全確保方法は既に説明したものと同じであるので、以下では証明局に用いる部分について丁寧に説明し他の部分については説明の重複を避けることにする。

第１の当事者Ｉと第２の当事者IIは、互いに合意した取引内容を電子情報化して保管する。しかし、電子化された文書は書き換えを行っても痕跡が残らないので原本性は保証できない。したがって、将来の争いの余地を小さくするため信頼を置くことができる第三者の機関である証明局ＣＡを利用して、取引内容を寄託しておき必要に応じて原本の提示を受けて確認するようにすることが要請される。

ところが、原本をフルテキストとして記録する場合は証明局ＣＡには極めて大きな記憶容量が必要となる。また、証明局ＣＡでも改竄を受ける可能性があり、

電子情報の真正性を完全に保証しようとすると証明局ＣＡの管理運営には大きな困難が付いて回ることになる。

本実施例は、本発明の電子情報安全確保方法を適用して構成したもので、証明局ＣＡの負担が小さくしかも高い確度で電子情報の原本性を保証する認証システムである。

当事者Ⅰ，Ⅱは相互の合意内容を前記実施例の方法に基づいて情報ブロックＡ，Ｂ，Ｃに分割する。第１当事者Ⅰは第１の情報ブロックＡを保管し、第２当事者Ⅱは第２の情報ブロックＣを保管する。さらに、第３の情報ブロックＢは証明局ＣＡに寄託する。

当事者間で合意内容に争いがあるときには、両当事者が保管して置いた情報ブロックＡ，Ｃと証明局ＣＡに寄託して置いた情報ブロックＢを統合し当初の合意文書の電子情報を正しく復元して、いずれの主張が正当であるかの認定をすることができる。

このような認証システムでは、いずれかの機関で記録を変成した場合には原本を復元することができない。したがって復元された電子情報は正しく原本の内容を伝えることになる。このため、証明局ＣＡは原本の極く一部を記録しておくだけで復元された電子情報の原本性を保証することができる。このように証明局ＣＡの有するべき記憶容量が小さくなり、また合意内容全文の保管をしなくても良いため証明局ＣＡとしての保管責任も緩和されることになる。

産業上の利用可能性

以上詳細に説明した通り、本発明の電子情報の安全確保方法は、電子情報ファイルを一旦情報エレメントに分割して再配置し情報ブロックに分納して通信路に置いたり記憶装置に納めるので、外部の者が通信途中や格納中の情報ブロックを窃取しても、小さな情報エレメントがバラバラに収納されていて電子情報の内容を判読することができず、秘密の漏洩を防ぐことができる。また、電子情報を復元する際に電子情報の原本性を容易に確認することができる。なお、受信者が通信路を介して受け取った通信結果や復元した電子情報ファイルを発信者まで返送して保存した写本と照合するようにしたものでは原本性を極めて高度に保証することができる。

請求の範囲

1．電子情報ファイルを複数の情報エレメントに分割し、分割された情報エレメントを選択し順序を変えて組み合わせることにより全ての情報ブロックを統合すると全ての情報エレメントが含まれるような1個以上の情報ブロックを生成し、また前記情報エレメントと情報ブロックの形成情報を記録した分割抽出データを生成し、該情報ブロックと分割抽出データを格納もしくは伝送し、該電子情報を使用するときにすべての前記情報ブロックと分割抽出データを集合して該分割抽出データに基づき前記情報ブロックに含まれる情報エレメントを再分割し正しい順序に並べ直して統合し、元の電子情報ファイルを復元することを特徴とする電子情報の安全確保方法。

2．前記分割抽出データを別途に格納もしくは送付することを特徴とする請求の範囲第1項記載の電子情報の安全確保方法。

3．前記各情報エレメントに係る前記分割抽出データを該情報エレメント毎に付帯させることを特徴とする請求の範囲第1項記載の電子情報の安全確保方法。

4．前記情報ブロックと分割抽出データを外部記憶装置に記憶して外部記憶装置における電子情報を安全に保管することを特徴とする請求の範囲第1項から第3項のいずれかに記載の電子情報の安全確保方法。

5．前記情報ブロックを複数形成し、該情報ブロックのそれぞれを分離した状態で前記分割抽出データと共に受信者に伝送することを特徴とする請求の範囲第1項から第3項のいずれかに記載の電子情報の安全確保方法。

6．前記分割抽出データに前記電子情報ファイルの原本性を確認するデータを含ませることを特徴とする請求の範囲第5項記載の電子情報の安全確保方法。

7．前記情報エレメントの内から選択した情報エレメントが複数の情報ブロックに共通して含まれるようにして、情報エレメントを統合するときに別々の情報ブロックに重複して含まれている前記情報エレメント同士の同一性を検証して情報の安全を確認することを特徴とする請求の範囲第1項から第6項のいずれかに記載の電子情報の安全性確保方法。

8．さらに、送付する電子情報の原本を保存し、受信者側で復元した電子情報を返送させ、前記電子情報原本と照合して同一性を確認することを特徴とする請求

の範囲第５項から第７項のいずれかに記載の電子情報の安全確保方法。

９．さらに、送付する電子情報の原本を保存し、受信者側で受信した情報ブロックを返送させ、前記電子情報原本と照合して同一性を確認することを特徴とする請求の範囲第５項から第７項のいずれかに記載の電子情報の安全確保方法。

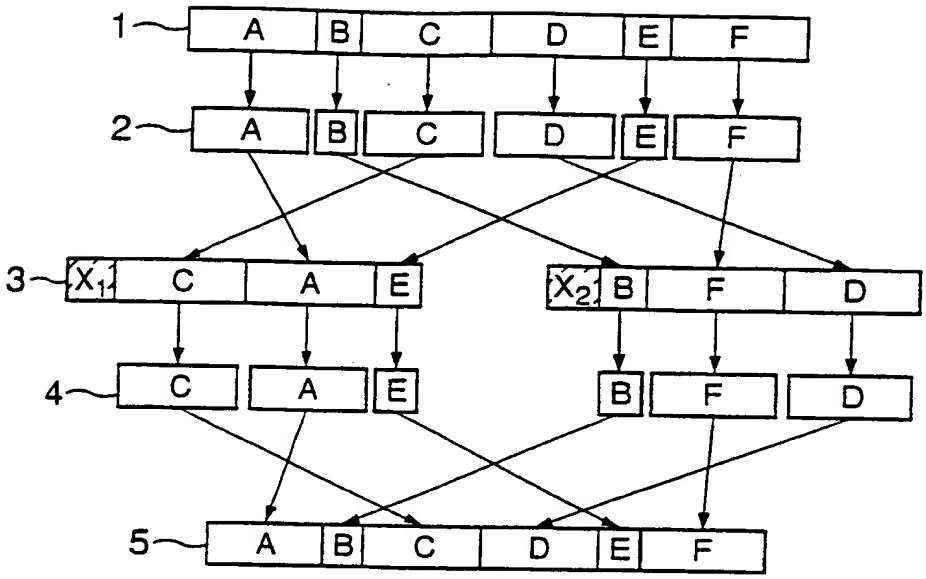
１０．前記情報ブロックおよび前記分割抽出データのうち少なくとも１個が他の電子情報の伝送手段と異なる第２の伝送手段により受信者に送付されることを特徴とする請求の範囲第５項から第９項のいずれかに記載の電子情報の安全確保方法。

１１．前記伝送手段または第２伝送手段には転送局を介在させて、該伝送手段で送る情報のブロックは宛先情報と共に情報パッケージに収容して該転送局に宛てて送付し、該転送局が該宛先情報に基づいて前記受信者に転送することを特徴とする請求の範囲第１０項記載の電子情報の安全確保方法。

１２．前記転送局が前記情報ブロックを前記受信者の請求があるまで格納保持していることを特徴とする請求の範囲第１１項記載の電子情報の安全確保方法。

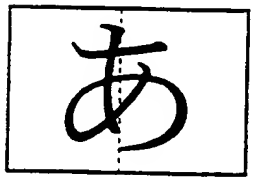
１３．電子情報ファイルを分割した前記情報ブロックを証明局と当事者がそれぞれ分かち持つようにして、該電子情報を使用するときに該証明局と該当事者とからすべての前記情報ブロックを収集して統合し、元の電子情報を復元することを特徴とする請求の範囲第１項から第１２項のいずれかに記載の電子情報の安全性確保方法。

第１図

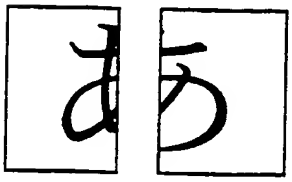


第２図

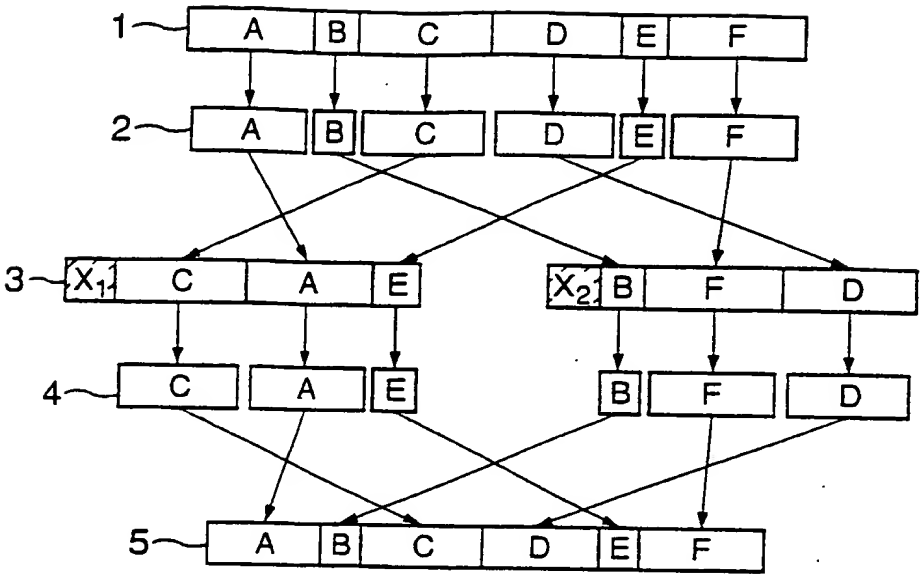
(a)



(b)

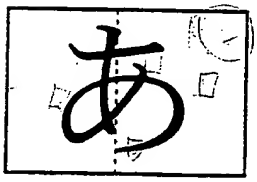


第１図

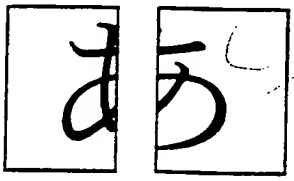


第２図

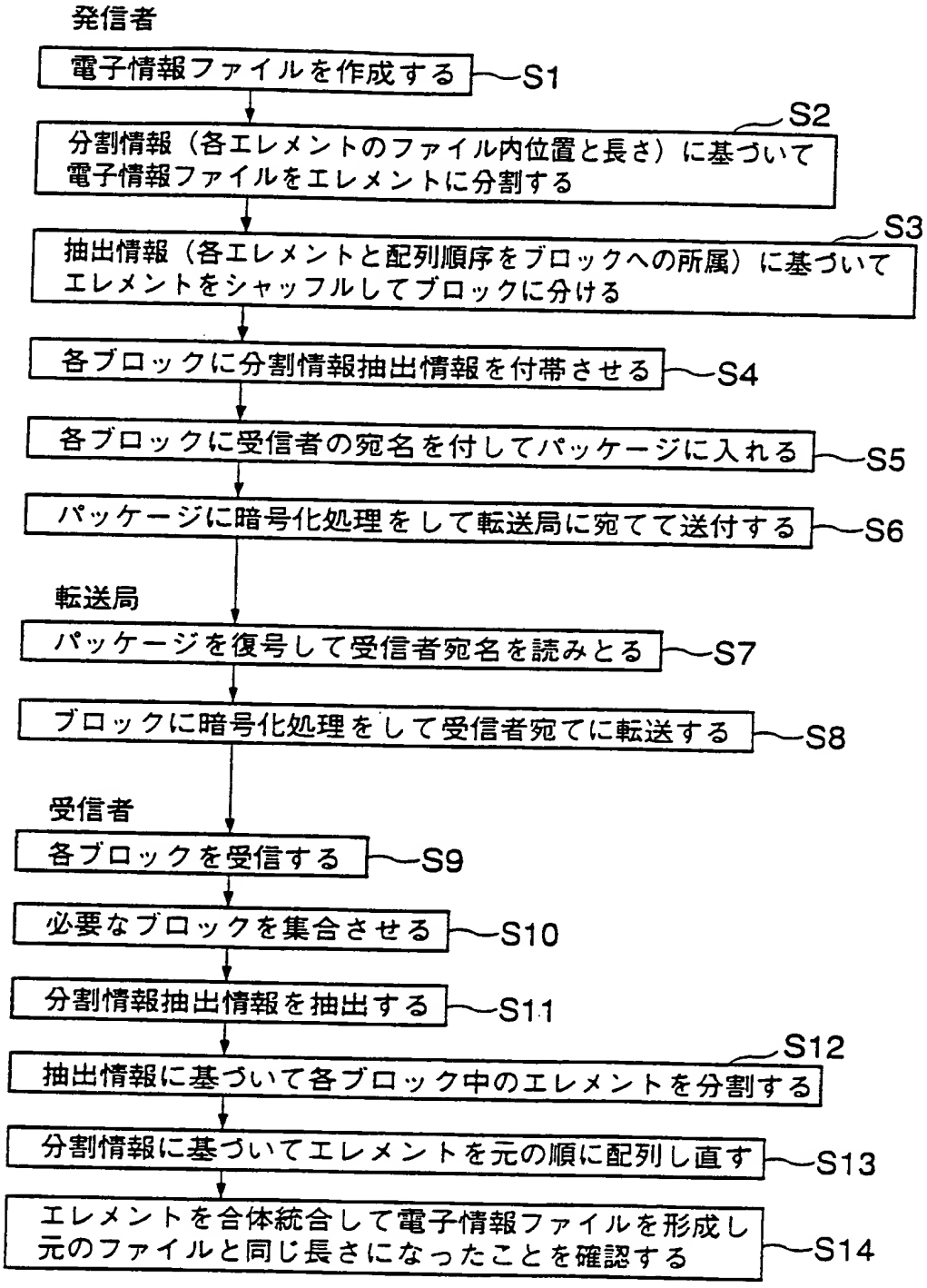
(a)



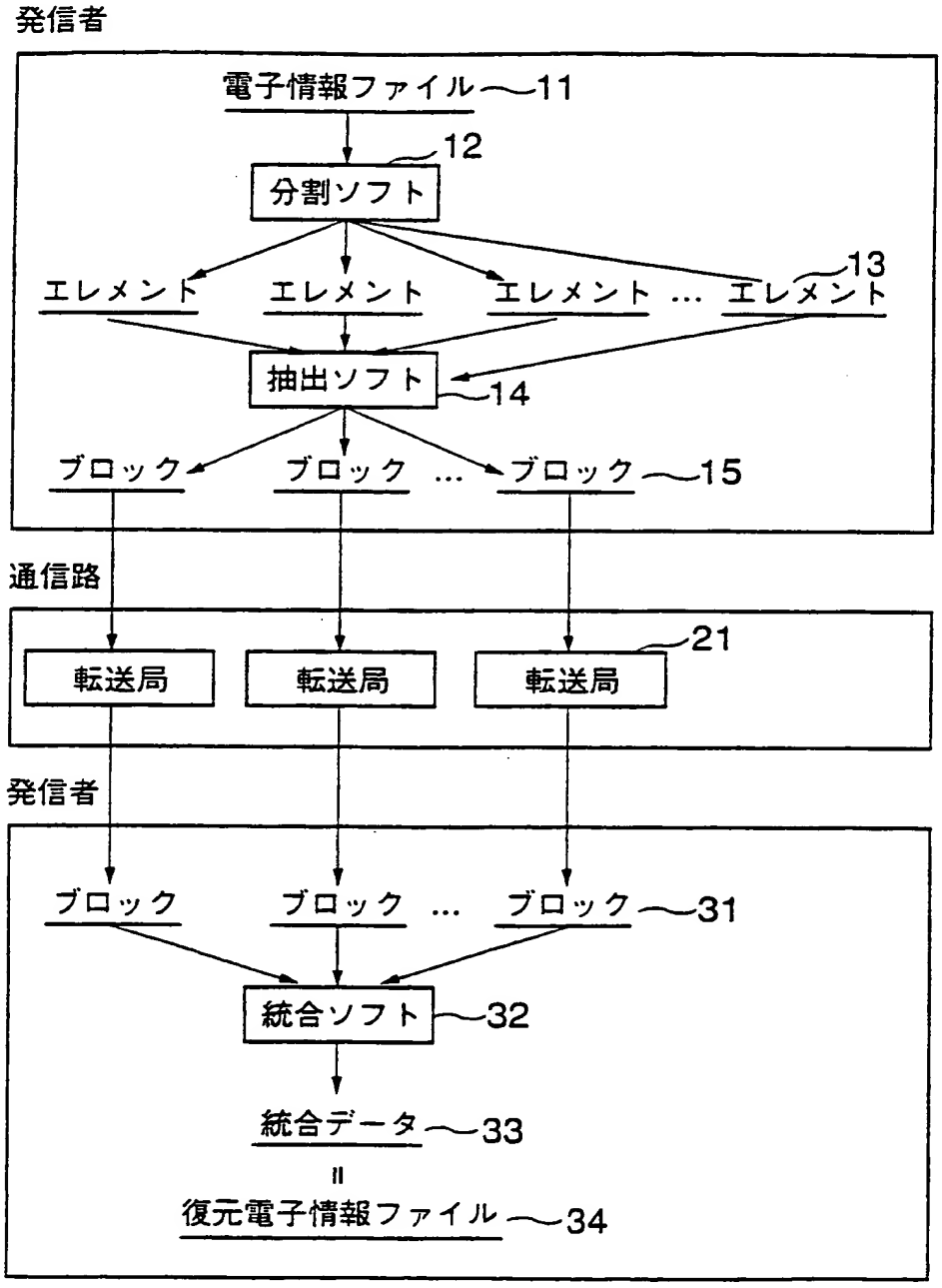
(b)



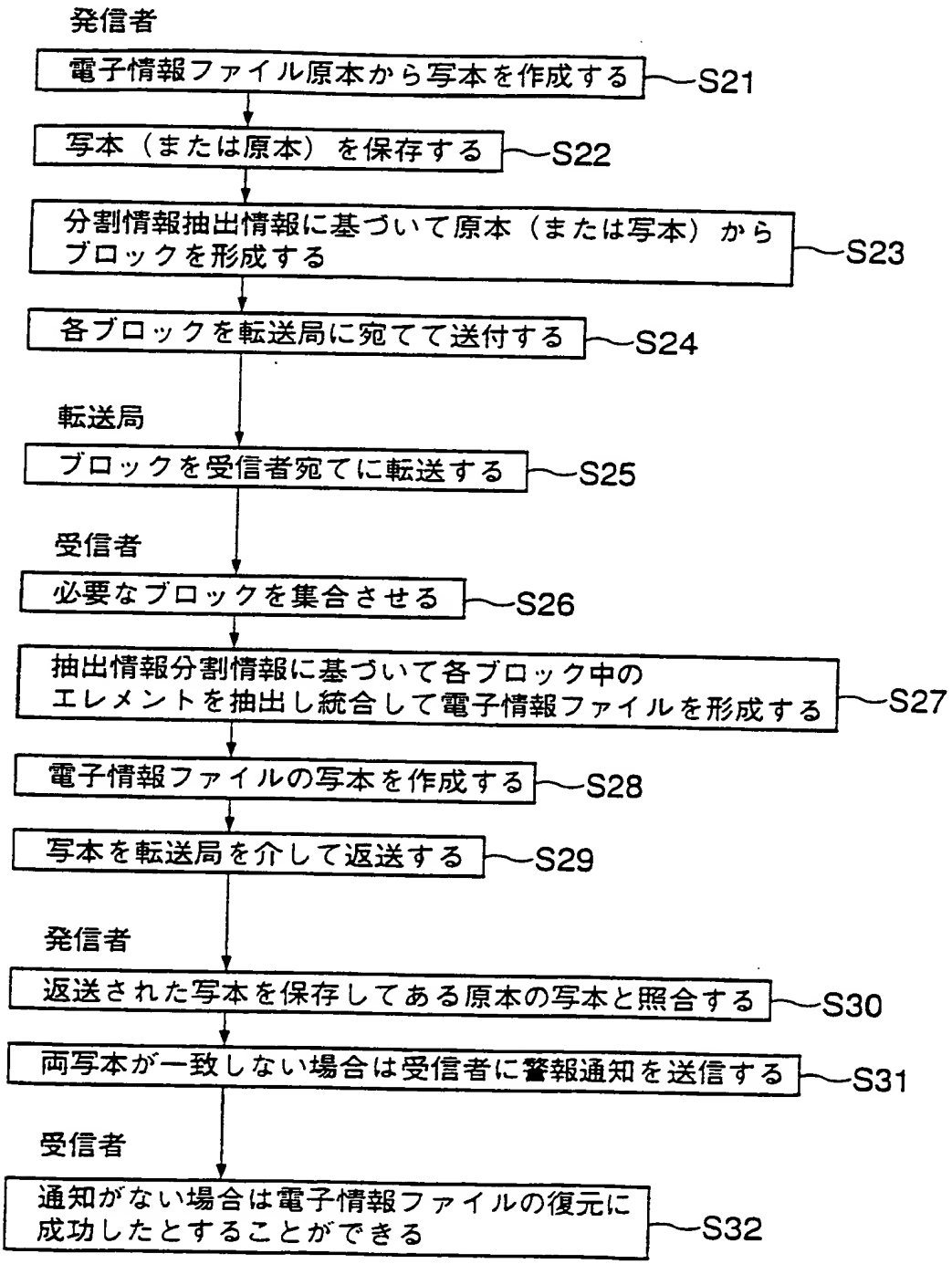
第３図


発信者
電子情報ファイルを作成する
S1
分割情報（各エレメントのファイル内位置と長さ）に基づいて電子情報ファイルをエレメントに分割する
S2
抽出情報（各エレメントと配列順序をブロックへの所属）に基づいてエレメントをシャッフルしてブロックに分ける
S3
各ブロックに分割情報抽出情報を付帯させる
S4
各ブロックに受信者の宛名を付してパッケージに入れる
S5
パッケージに暗号化処理をして転送局に宛てて送付する
S6
転送局
パッケージを復号して受信者宛名を読みとる
S7
ブロックに暗号化処理をして受信者宛てに転送する
S8
受信者
各ブロックを受信する
S9
必要なブロックを集合させる
S10
分割情報抽出情報を抽出する
S11
抽出情報に基づいて各ブロック中のエレメントを分割する
S12
分割情報に基づいてエレメントを元の順に配列し直す
S13
エレメントを合体統合して電子情報ファイルを形成し元のファイルと同じ長さになったことを確認する
S14

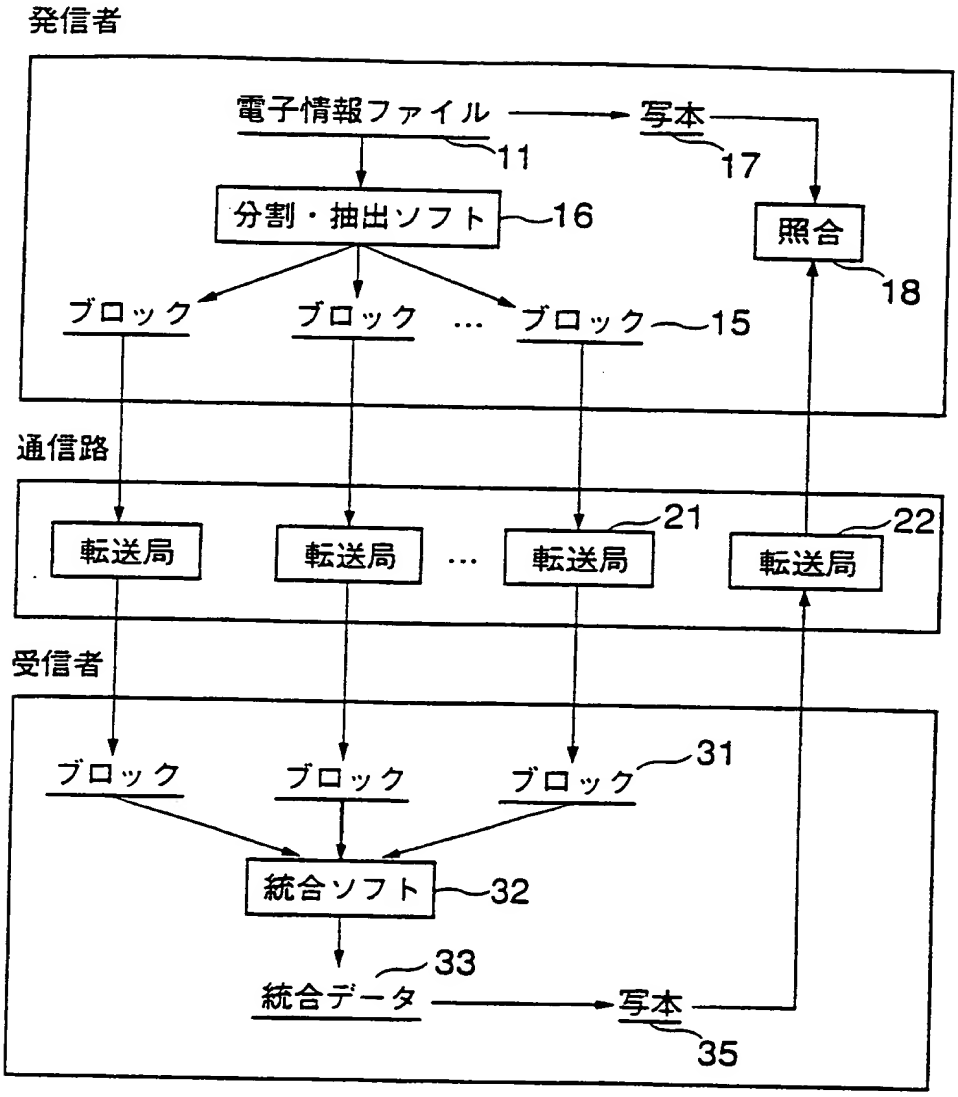
第４図


発信者
電子情報ファイル
11
12
分割ソフト
エレメント
エレメント
エレメント
エレメント
13
抽出ソフト
14
ブロック
ブロック
ブロック
15
通信路
転送局
転送局
転送局
21
発信者
ブロック
ブロック
ブロック
31
統合ソフト
32
統合データ
33
復元電子情報ファイル
34

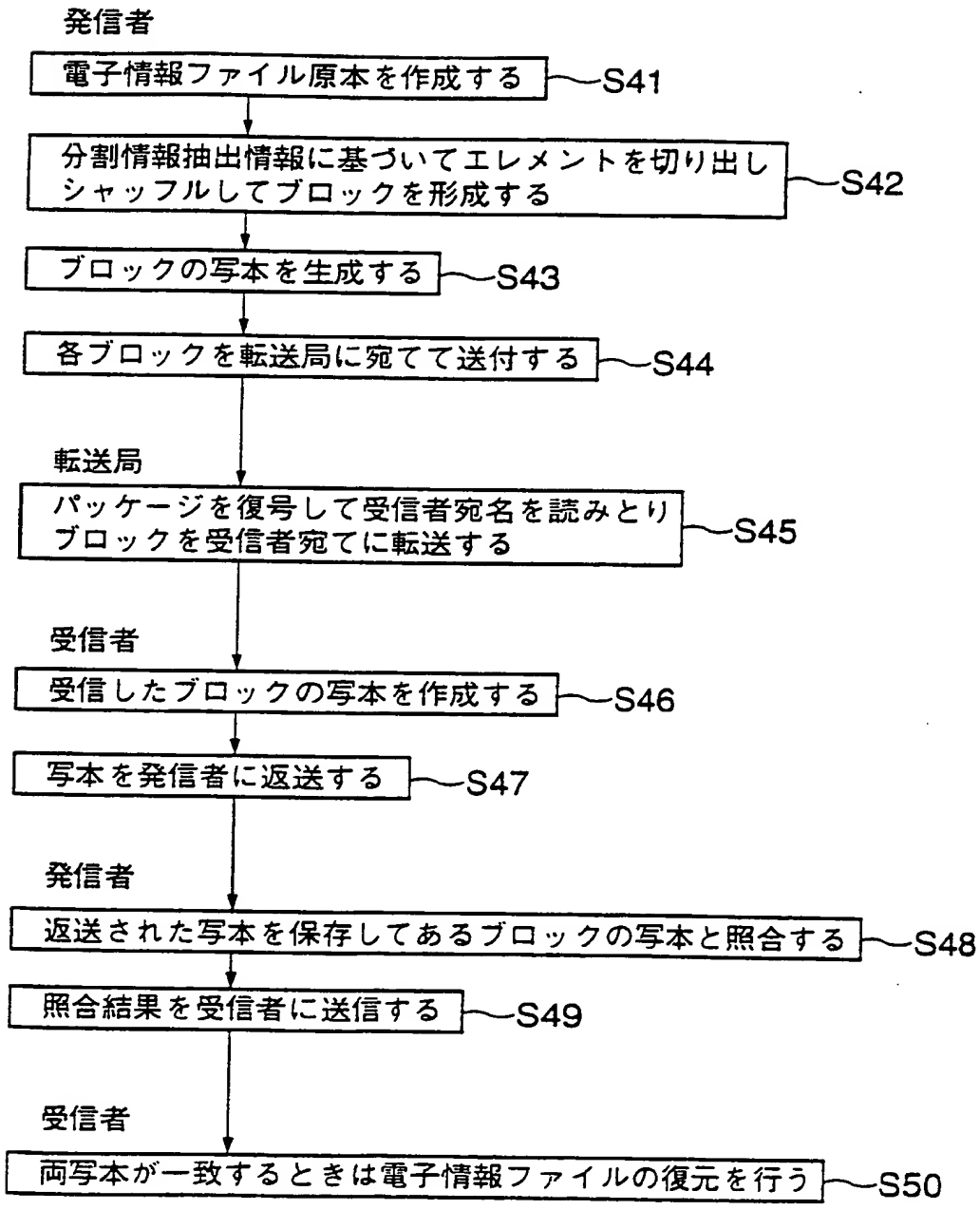
第５図


発信者
電子情報ファイル原本から写本を作成する
S21
写本（または原本）を保存する
S22
分割情報抽出情報に基づいて原本（または写本）から
ブロックを形成する
S23
各ブロックを転送局に宛てて送付する
S24
転送局
ブロックを受信者宛てに転送する
S25
受信者
必要なブロックを集合させる
S26
抽出情報分割情報に基づいて各ブロック中の
エレメントを抽出し統合して電子情報ファイルを形成する
S27
電子情報ファイルの写本を作成する
S28
写本を転送局を介して返送する
S29
発信者
返送された写本を保存してある原本の写本と照合する
S30
両写本が一致しない場合は受信者に警報通知を送信する
S31
受信者
通知がない場合は電子情報ファイルの復元に
成功したとすることができる
S32

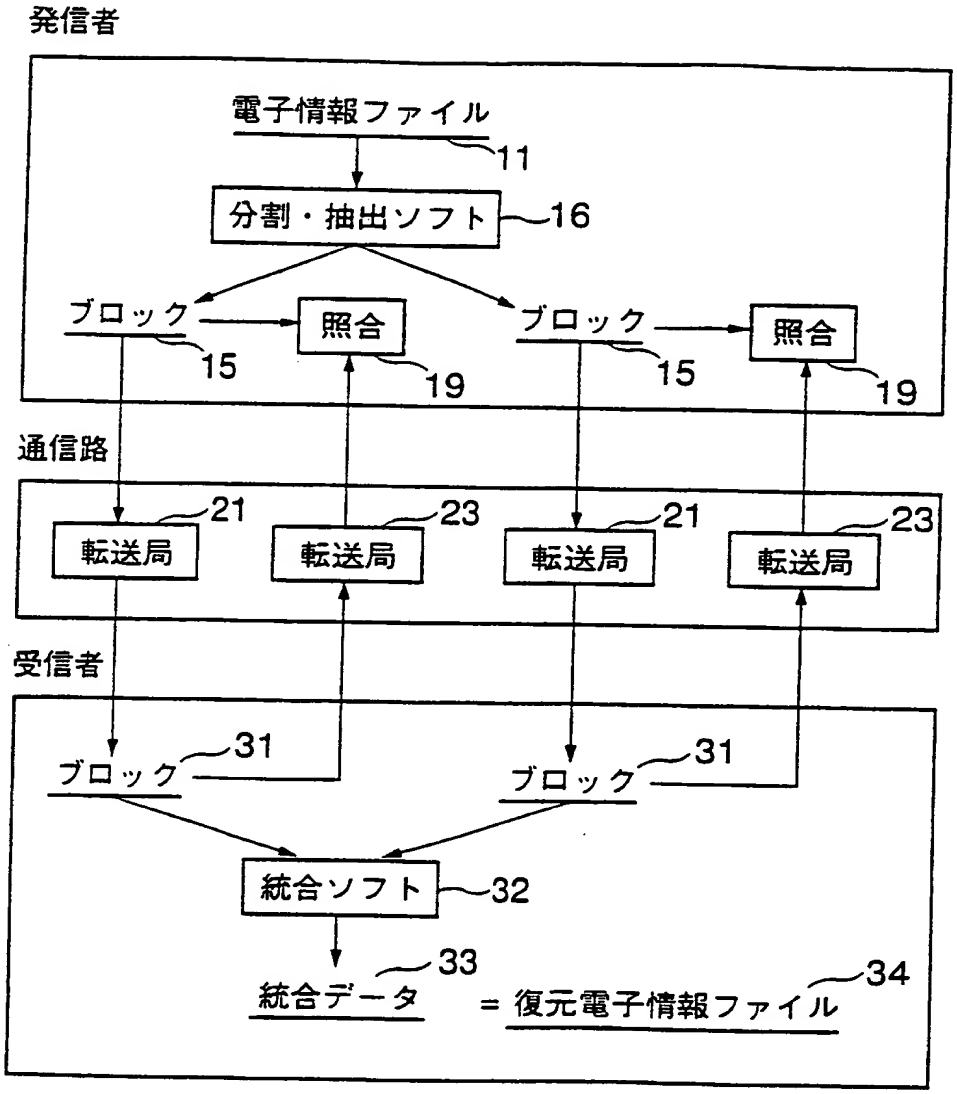
第６図


発信者
電子情報ファイル
11
写本
17
分割・抽出ソフト
16
照合
18
ブロック
ブロック
…
ブロック
15
通信路
転送局
転送局
…
転送局
21
転送局
22
受信者
ブロック
ブロック
ブロック
31
統合ソフト
32
33
統合データ
写本
35

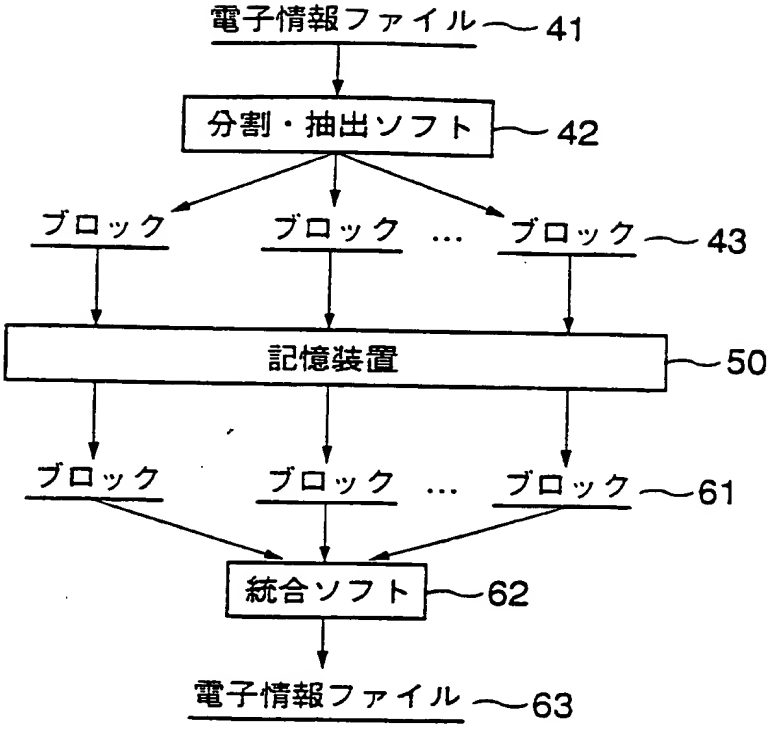
第７図


発信者
電子情報ファイル原本を作成する
S41
分割情報抽出情報に基づいてエレメントを切り出し
シャッフルしてブロックを形成する
S42
ブロックの写本を生成する
S43
各ブロックを転送局に宛てて送付する
S44
転送局
パッケージを復号して受信者宛名を読みとり
ブロックを受信者宛てに転送する
S45
受信者
受信したブロックの写本を作成する
S46
写本を発信者に返送する
S47
発信者
返送された写本を保存してあるブロックの写本と照合する
S48
照合結果を受信者に送信する
S49
受信者
両写本が一致するときは電子情報ファイルの復元を行う
S50

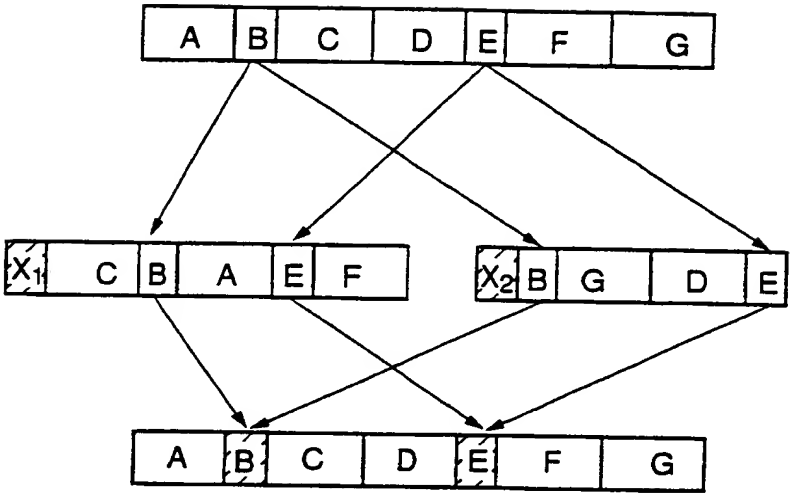
第８図


発信者
電子情報ファイル
11
分割・抽出ソフト
16
ブロック
15
照合
19
ブロック
15
照合
19
通信路
転送局
21
転送局
23
転送局
21
転送局
23
受信者
ブロック
31
ブロック
31
統合ソフト
32
統合データ
33
＝復元電子情報ファイル
34

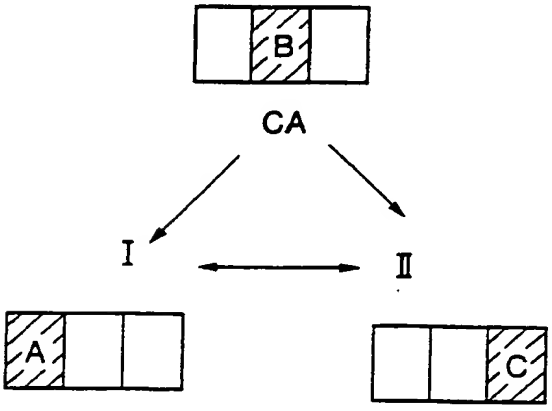
第９図


電子情報ファイル
41
分割・抽出ソフト
42
ブロック
ブロック
…
ブロック
43
記憶装置
50
ブロック
ブロック
…
ブロック
61
統合ソフト
62
電子情報ファイル
63

第１０図



第１１図



INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/01350

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] G09C1/04, G09C1/00, H04L9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] G09C1/04, G09C1/00, H04L9/32

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 2-259689, A (Matsushita Electric Industrial Co., Ltd.), 22 October, 1990 (22. 10. 90), Full text ; Figs. 1 to 6 (Family: none)	1-13
Y	JP, 60-247683, A (Mitsubishi Electric Corp.), 7 December, 1985 (07. 12. 85), Page 1, lower right column, line 2 to page 2, upper left column, line 9 ; Figs. 1 to 3 (Family: none)	4, 11-13
Y	JP, 63-225840, A (Yokogawa-Hewlett-Packard, Ltd.), 20 September, 1988 (20. 09. 88), Page 2, lower left column, line 19 to page 3, lower right column, line 1 ; Figs. 1 to 6 & GB, 8704883, A & EP, 281225, A & US, 4933969, A & DE, 3889561, C	6-9

[x] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
1 June, 1999 (01. 06. 99)

Date of mailing of the international search report
15 June, 1999 (15. 06. 99)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/01350

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 3-151738, A (Hitachi,Ltd.), 27 June, 1991 (27. 06. 91), Page 4, upper left column, lines 14 to 20, page 4, lower right column, line 15 to page 5, upper right column, line 10 ; Figs. 1 to 9 (Family: none)	6-9
Y	JP, 8-185376, A (Hitachi,Ltd.), 16 July, 1996 (16. 07. 96), Page 2, column 2, lines 3 to 36, page 3, column 3, lines 2 to 7 ; page 6, column 10, line 18 to page 7, column 11, line 22 (Family: none)	13
A	JP, 10-91705, A (Hitachi,Ltd.), 10 April, 1998 (10. 04. 98), Page 2, column 2, line 49 to page 3, column 3, line 42 (Family: none)	1-13
A	JP, 62-72243, A (Fujitsu Ltd.), 2 April, 1987 (02. 04. 87), Page 1, lower right column, lines 5 to 10 ; page 2, upper left column, lines 15 to 17 ; Figs. 1, 2 (Family: none)	1-13